Bitcoin

Contents

1 Overview 1

1.1 Bitcoin . . . 1

1.1.1 Etymology and orthography . . . 1

1.1.2 Design . . . 1

1.1.3 History . . . 5

1.1.4 Economics . . . 6

1.1.5 Legal status and regulation . . . 11

1.1.6 Criminal activity . . . 11

1.1.7 Security . . . 13

1.1.8 Data in the blockchain . . . 14

1.1.9 In academia . . . 14

1.1.10 In art, entertainment, and media . . . 14

1.1.11 See also . . . 14

1.1.12 Notes . . . 14

1.1.13 References . . . 15

1.2 History of Bitcoin . . . 26

1.2.1 Pre-history . . . 26

1.2.2 Creation . . . 26

1.2.3 Growth . . . 26

1.2.4 Prices and value history . . . 27

1.2.5 Satoshi Nakamoto . . . 28

1.2.6 The fork of March 2013 . . . 28

1.2.7 Regulatory issues . . . 29

1.2.8 Theft and exchange shutdowns . . . 29

1.2.9 Taxation and regulation . . . 30

1.2.10 Sports sponsorship . . . 31

1.2.11 References . . . 31

1.2.12 External Links . . . 35

1.3 Legality of bitcoin by country . . . 35

1.3.1 List by country . . . 35

1.3.2 Details by country . . . 35

1.3.3 Footnotes . . . 41

1.3.4 References 42

2 People 47

2.1 Satoshi Nakamoto 47

2.1.1 Development of bitcoin 47

2.1.2 Characteristics 47

2.1.3 Candidates 47

2.1.4 References 49

2.1.5 External links 51

2.2 Hal Finney 51

2.2.1 Early life and education 51

2.2.2 Career 51

2.2.3 Private life, illness 51

2.2.4 Death 51

2.2.5 References 51

2.2.6 External links 52

2.3 Gavin Andresen 52

2.3.1 References 52

2.3.2 External links 52

2.4 Nick Szabo 52

2.4.1 Bit gold 53

2.4.2 Bitcoin speculation 53

2.4.3 References 53

2.4.4 External links 54

2.5 Winklevoss twins 54

2.5.1 Early life and education 54

2.5.2 ConnectU 54

2.5.3 Bitcoin 54

2.5.4 Popular culture 55

2.5.5 References 55

2.6 Mark Karpelès 55

2.6.1 Early life and education 55

2.6.2 Career 56

2.6.3 Arrest and prosecution 56

2.6.4 References 56

2.6.5 External links 57

3 Organizations 58

3.1 Bitcoin Foundation 58

3.1.1 History 58

3.1.2 Leadership 58

3.1.3 Awards 58

3.1.4 Criticism 58
3.1.5 References 59
3.1.6 External links 60

4 Technologies 61
4.1 Bitcoin network 61
4.1.1 Transactions 61
4.1.2 Mining 61
4.1.3 Local system resources 62
4.1.4 Payment verification 63
4.1.5 See also 63
4.1.6 References 63
4.2 Cryptocurrency 63
4.2.1 Overview 63
4.2.2 History 64
4.2.3 Legality 64
4.2.4 Timestamping 66
4.2.5 Economics 66
4.2.6 List 67
4.2.7 Academic studies 67
4.2.8 Criticism 67
4.2.9 See also 67
4.2.10 References 68
4.2.11 Further reading 70
4.2.12 External links 70
4.3 Elliptic Curve Digital Signature Algorithm 70
4.3.1 Key and signature-size comparison to DSA 70
4.3.2 Signature generation algorithm 70
4.3.3 Signature verification algorithm 70
4.3.4 Correctness of the algorithm 71
4.3.5 Security 71
4.3.6 See also 71
4.3.7 Notes 71
4.3.8 References 72
4.3.9 External links 72
4.4 Peer-to-peer 72
4.4.1 Historical development 73
4.4.2 Architecture 73
4.4.3 Applications 76
4.4.4 Social implications 77
4.4.5 Political implications 77
4.4.6 Current research 78

4.4.7 See also . . . 78
4.4.8 References . . . 78
4.4.9 External links . . . 80
4.5 Proof-of-work system . . . 81
4.5.1 Background . . . 81
4.5.2 Variants . . . 81
4.5.3 List of proof-of-work functions . . . 82
4.5.4 Reusable proof-of-work as e-money . . . 82
4.5.5 Notes . . . 83
4.5.6 See also . . . 83
4.5.7 References . . . 83
4.5.8 External links . . . 83
4.6 SHA-2 . . . 84
4.6.1 Hash standard . . . 84
4.6.2 Applications . . . 85
4.6.3 Cryptoanalysis and validation . . . 85
4.6.4 Test vectors . . . 86
4.6.5 Pseudocode . . . 86
4.6.6 Comparison of SHA functions . . . 88
4.6.7 See also . . . 89
4.6.8 References . . . 89
4.6.9 External links . . . 90

5 Exchanges 91

5.1 ANX (Hong Kong company) . . . 91
5.1.1 Sub-brands . . . 91
5.1.2 History . . . 91
5.1.3 Company Growth . . . 91
5.1.4 Acquisitions . . . 92
5.1.5 Agreements . . . 92
5.1.6 References . . . 92
5.2 BitInstant . . . 93
5.2.1 History . . . 93
5.2.2 Criticism . . . 93
5.2.3 References . . . 93
5.2.4 External links . . . 94
5.3 Bitstamp . . . 94
5.3.1 Service disruptions . . . 94
5.3.2 Notes . . . 94
5.3.3 References . . . 95
5.3.4 External links . . . 95
5.4 BTC-e . . . 95

5.4.1 History 95

5.4.2 References 95

5.5 BTC China 95

5.5.1 History 96

5.5.2 References 96

5.5.3 External links 96

5.6 Buttercoin 96

5.6.1 Funding 96

5.6.2 References 96

5.6.3 External links 96

5.7 Coinbase 96

5.7.1 History 97

5.7.2 Products 97

5.7.3 See also 97

5.7.4 References 97

5.8 Huobi 98

5.8.1 References 98

5.9 ItBit 98

5.9.1 References 99

5.10 LocalBitcoins 99

5.10.1 References 99

5.10.2 External links 99

5.11 Mt. Gox 99

5.11.1 Founding 99

5.11.2 2011 100

5.11.3 2013 100

5.11.4 Insolvency and shutdown 100

5.11.5 Legal action 101

5.11.6 See also 101

5.11.7 References 101

5.11.8 External links 103

5.12 OKCoin 103

5.12.1 History 104

5.12.2 Controversy 104

5.12.3 References 104

5.12.4 External links 104

6 Text and image sources, contributors, and licenses 105

6.1 Text 105

6.2 Images 111

6.3 Content license 116

Chapter 1

Overview

1.1 Bitcoin

Bitcoin is a digital asset[10] and a payment system[11] created by an unidentified programmer, or group of programmers,[12] under the name of Satoshi Nakamoto.[13] Bitcoin was introduced on 31 October 2008 to a cryptography mailing list,[14] and released as open-source software in 2009.[15] There have been several high-profile claims to the identity of Satoshi Nakamoto; however, none of them have provided proof beyond doubt that back up their claims.[13] The system is peer-to-peer and transactions take place between users directly, without an intermediary.[11]:4 These transactions are verified by network nodes and recorded in a public distributed ledger called the *blockchain*,[16] which uses bitcoin as its unit of account. Since the system works without a central repository or single administrator, the U.S. Treasury categorizes bitcoin as a decentralized virtual currency.[1] Bitcoin is often called the first cryptocurrency,[17][18][19] although prior systems existed[note 5] and it is more correctly described as the first decentralized digital currency.[11][23] Bitcoin is the largest of its kind in terms of total market value.[24]

Bitcoins are created as a reward for payment processing work in which users offer their computing power to verify and record payments into a public ledger. This activity is called *mining* and miners are rewarded with transaction fees and newly created bitcoins.[11] Besides being obtained by mining, bitcoins can be exchanged for other currencies,[25] products, and services.[26] When sending bitcoins, users can pay an optional transaction fee to the miners.[27]

In February 2015, the number of merchants accepting bitcoin for products and services passed 100,000.[28] Instead of 2–3% typically imposed by credit card processors, merchants accepting bitcoins often pay fees in the range from 0% to less than 2%.[29] Despite the fourfold increase in the number of merchants accepting bitcoin in 2014, the cryptocurrency did not have much momentum in retail transactions.[30] The European Banking Authority[31] and other sources[11]:11 have warned that bitcoin users are not protected by refund rights or chargebacks. The use of bitcoin by criminals has attracted the attention of financial regulators,[32] legislative bodies,[33] law enforcement,[34] and media.[35] Criminal activities are primarily centered around darknet markets and theft, though officials in countries such as the United States also recognize that bitcoin can provide legitimate financial services.[33]

1.1.1 Etymology and orthography

The word *bitcoin* occurred in the white paper that defined bitcoin published in 2008. It is a compound of the words *bit* and *coin*.[36] The white paper frequently uses the shorter *coin*.[37]

There is no uniform convention for *bitcoin* capitalization. Some sources use *Bitcoin*, capitalized, to refer to the technology and network and *bitcoin*, lowercase, to refer to the unit of account.[38] *The Wall Street Journal*,[39] *The Chronicle of Higher Education*,[40] and the *Oxford English Dictionary*[36] advocate use of lowercase *bitcoin* in all cases. This article follows the latter convention.

1.1.2 Design

Blockchain

See also: Blockchain (database)

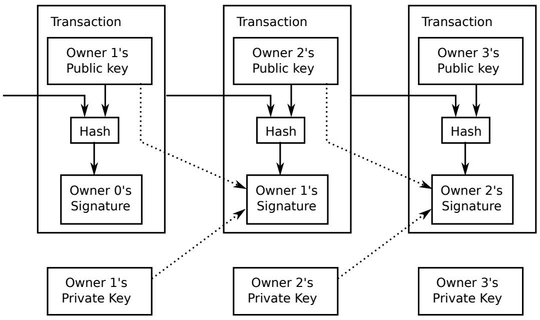
The *blockchain* is a public ledger that records bitcoin transactions.[41] A novel solution accomplishes this without any trusted central authority: maintenance of the blockchain is performed by a network of communicating nodes running bitcoin software.[11] Transactions of the form *payer X sends Y bitcoins to payee Z* are broadcast to this network using readily available software applications.[42] Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes. The blockchain is a distributed database – to achieve independent verification of the chain of ownership of any and every bitcoin (amount), each network node stores its own copy of the blockchain.[18] Approximately six times per hour, a new group of accepted transactions, a block, is created, added to the blockchain, and quickly published to all nodes. This allows bitcoin software to determine when a particular bitcoin amount has been spent, which is necessary in order to prevent double-spending in an environment without central oversight. Whereas a conventional ledger records the transfers of actual bills or promissory notes that exist apart from it, the blockchain is the only place that bitcoins can be said to exist in the form of unspent outputs of transactions.[43]

Units

The unit of account of the bitcoin system is bitcoin. As of 2014, symbols used to represent bitcoin are BTC,[note 2] XBT,[note 3] and ฿.[note 4][44]:2 Small amounts of bitcoin used as alternative units are millibitcoin (mBTC), microbitcoin (µBTC), and satoshi. Named in homage to bitcoin's creator, a *satoshi* is the smallest amount within bitcoin representing 0.00000001 bitcoin, one hundred millionth of a bitcoin.[4] A *millibitcoin* equals to 0.001 bitcoin, one thousandth of bitcoin.[45] One *microbitcoin* equals to 0.000001 bitcoin, one millionth of a bitcoin. A microbitcoin is sometimes referred to as a *bit*.

A proposal was submitted to the Unicode Consortium in October 2015 to add a codepoint for the symbol.[8] It is in the pipeline for position 20BF (⍰) in the Currency Symbols block.

Ownership



Simplified chain of ownership.[37] In reality, a transaction can have more than one input and more than one output.

Ownership of bitcoins implies that a user can spend bitcoins associated with a specific address. To do so, a payer must digitally sign the transaction using the corresponding private key. Without knowledge of the private key, the transaction cannot be signed and bitcoins cannot be spent. The network verifies the signature using the public key.[43]:ch. 5

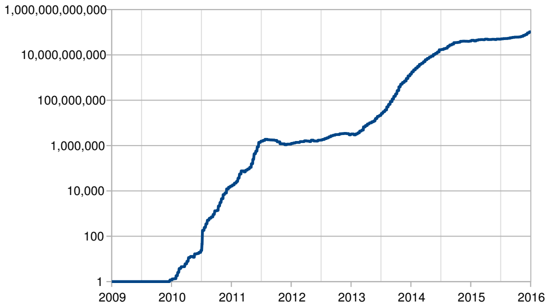
If the private key is lost, the bitcoin network will not recognize any other evidence of ownership;[11] the coins are then unusable, and thus effectively lost. For example, in 2013 one user claimed to have lost 7,500 bitcoins, worth $7.5 million at the time, when he accidentally discarded a hard drive containing his private key.[46]

Transactions

See also: Bitcoin network

A transaction must have one or more inputs.[27] For the transaction to be valid, every input must be an unspent output of a previous transaction. Every input must be digitally signed. The use of multiple inputs corresponds to the use of multiple coins in a cash transaction. A transaction can also have multiple outputs, allowing one to make multiple payments in one go. A transaction output can be specified as an arbitrary multiple of satoshi. As in a cash transaction, the sum of inputs (coins used to pay) can exceed the intended sum of payments. In such a case, an additional output is used, returning the change back to the payer.[27] Any input satoshis not accounted for in the transaction outputs become the transaction fee.[27]

Mining



Relative mining difficulty,[note 6] the scale is logarithmic.[47]

A mining farm in Iceland

Mining is a record-keeping service.[note 7] Miners keep the blockchain consistent, complete, and unalterable by repeatedly verifying and collecting newly broadcast transactions into a new group of transactions called a *block*.[49] Each block contains a cryptographic hash of the previous block,[49] using the SHA-256 hashing algorithm,[43]:ch. 7 which links it to the previous block[49] thus giving the blockchain its name.

In order to be accepted by the rest of the network, a new block must contain a so-called *proof-of-work*.[49] The proof-of-work requires miners to find a number called a *nonce*, such that when the block content is hashed along with the nonce, the result is numerically smaller than the network's *difficulty target*.[43]:ch. 8 This proof is easy for any node in the network to verify, but extremely time-consuming to generate, as for a secure cryptographic hash, miners must try many different nonce values (usually the sequence of tested values is 0, 1, 2, 3, …[43]:ch. 8) before meeting the difficulty target.

Every 2016 blocks (approximately 14 days), the difficulty target is adjusted based on the network's recent performance, with the aim of keeping the average time between new blocks at ten minutes. In this way the system automatically adapts to the total amount of mining power on the network.[43]:ch. 8

Between 1 March 2014 and 1 March 2015, the average number of nonces miners had to try before creating a new block increased from 16.4 quintillion to 200.5 quintillion.[50]

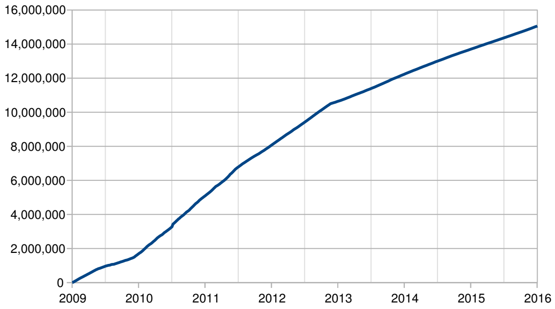
The proof-of-work system, alongside the chaining of blocks, makes modifications of the blockchain extremely hard, as an attacker must modify all subsequent blocks in order for the modifications of one block to be accepted.[51] As new blocks are mined all the time, the difficulty of modifying a block increases as time passes and the number of subsequent blocks (also called *confirmations* of the given block) increases.[49]

Practicalities It has become common for miners to join mining pools,[52] which combine the computational resources of their members in order to increase the frequency of generating new blocks. The reward for each block is then split proportionately among the members, creating a more predictable stream of income for each miner without necessarily changing their long-term average income,[53] although a fee may be charged for the service.[54][55]

The rewards of mining have led to ever-more-specialized technology being utilized. The most efficient mining hardware makes use of custom designed application-specific integrated circuits, which outperform general-purpose CPUs while using less power.[56] As of 2015, a miner who is not using purpose-built hardware is unlikely to earn enough to cover the cost of the electricity used in their efforts, even if they are a member of a pool.[57]

Energy consumption In 2013, electricity use was estimated to be 0.36 terawatt-hours per year or the equivalent of powering 31,000 US homes.[58] In 2014, it was estimated that specialized computers mining bitcoins required 0.1 to 10 GW of power.[59] As of 2015, even if all miners used energy-efficient processors, the combined electricity consumption would be 1.46 terawatt-hours per year—equal to the consumption of about 135,000 American homes.[60] Bitcoin miners have set up in places like Iceland where geothermal energy is cheap and cooling Arctic air is free.[61]

Supply



Total bitcoins in circulation.[47]

The successful miner finding the new block is rewarded with newly created bitcoins and transaction fees.[62] As of 9 July 2016,[63] the reward amounted to 12.5 newly created bitcoins per block added to the blockchain. To claim the reward, a special transaction called a *coinbase* is included with the processed payments.[43]:ch. 8 All bitcoins in existence have been created in such coinbase transactions. The bitcoin protocol specifies that the reward for adding a block will be halved every 210,000 blocks (approximately every four years). Eventually, the reward will decrease to zero, and the limit of 21 million bitcoins[note 8] will be reached c. 2140; the record keeping will then be rewarded by transaction fees solely.[64]

In other words, bitcoin's inventor Nakamoto set a monetary policy at the start of the bitcoin concept that there would only ever be 21 million bitcoins in total, their numbers being released roughly every ten minutes, and the rate at which they would be generated would drop by half every four years until all were in circulation.[65]

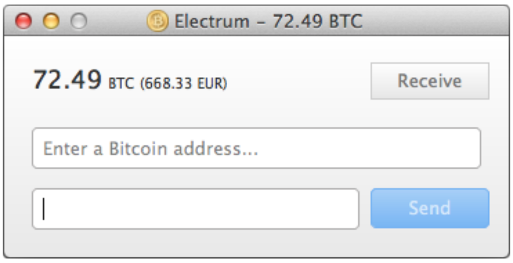
Transaction fees

Paying a transaction fee is optional.[27] Miners can choose which transactions to process[27] and prioritize those that pay higher fees. Fees are based on the storage size of the transaction generated, which in turn is dependent on the number of inputs used to create the transaction. Furthermore, priority is given to older unspent inputs.[43]:ch. 8

Wallets

See also: Digital wallet

A *wallet* stores the information necessary to transact bitcoins. While wallets are often described as a place to hold[66] or store bitcoins,[67] due to the nature of the system, bitcoins are inseparable from the blockchain transaction ledger. A better way to describe a wallet is something that "stores the digital credentials for your bit-



Electrum bitcoin wallet

Bitcoin paper wallet generated at bitaddress.org

Trezor hardware wallet

coin holdings”[67] and allows you to access (and spend) them. Bitcoin uses public-key cryptography, in which two cryptographic keys, one public and one private, are generated.[68] At its most basic, a wallet is a collection of these keys.

There are several types of wallets. *Software wallets* connect to the network and allow spending bitcoins in addition to holding the credentials that prove ownership.[69] Software wallets can be split further in two categories: full clients and lightweight clients.

- **Full clients** verify transactions directly on a local copy of the blockchain (over 65 GB as of April 2016[70]). Because of its size / complexity, the entire blockchain is not suitable for all computing devices.
- **Lightweight clients** on the other hand consult a full client to send and receive transactions without requiring a local copy of the entire blockchain (see simplified payment verification – SPV). This makes lightweight clients much faster to setup and allows them to be used on low-power, low-bandwidth devices such as smartphones. When using a lightweight wallet however, the user must trust the server to a certain degree. When using a lightweight client, the server can not steal bitcoins, but it can report faulty values back to the user. With both types of software wallets, the users are responsible for keeping their private keys in a secure place.[71]

Besides software wallets, Internet services called *online wallets* offer similar functionality but may be easier to use. In this case, credentials to access funds are stored with the online wallet provider rather than on the user’s hardware.[72][73] As a result, the user must have complete trust in the wallet provider. A malicious provider or a breach in server security may cause entrusted bitcoins to be stolen. An example of such security breach occurred with Mt. Gox in 2011.[74]

Physical wallets also exist and are more secure, as they store the credentials necessary to spend bitcoins offline.[67] Examples combine a novelty coin with these credentials printed on metal,[75] Others are simply paper printouts. Another type of wallet called a *hardware wallet* keeps credentials offline while facilitating transactions.[76]

Reference implementation The first wallet program was released in 2009 by Satoshi Nakamoto as open-source code.[15] Sometimes referred to as the “Satoshi client,” this is also known as the reference client because it serves to define the bitcoin protocol and acts as a standard for other implementations.[69] In version 0.5 the client moved from the wxWidgets user interface toolkit to Qt, and the whole bundle was referred to as Bitcoin-Qt.[69] After the release of version 0.9, the software bundle was renamed Bitcoin Core to distinguish itself from the network.[77][78] Today, other forks of Bitcoin Core exist such as Bitcoin XT and Bitcoin Classic.

Privacy

Bitcoin is a pseudonymous currency, meaning that funds are not tied to real-world entities but rather bitcoin addresses. Owners of bitcoin addresses are not explicitly identified, but all transactions on the blockchain are public. In addition, transactions can be linked to individuals and companies through “idioms of use” (e.g., transactions that spend coins from multiple inputs indicate that the inputs may have a common owner) and corroborating public transaction data with known information on owners of certain addresses.[79] Additionally, bitcoin exchanges, where bitcoins are traded for traditional currencies, may be required by law to collect personal information.[80]

To heighten financial privacy, a new bitcoin address can be generated for each transaction.[81] For example, hierarchical deterministic wallets generate pseudorandom “rolling addresses” for every transaction from a single seed, while only requiring a single passphrase to be remembered to recover all corresponding private keys.[82] Additionally, “mixing” and CoinJoin services aggregate multiple users’ coins and output them to fresh addresses to increase privacy.[83] Researchers at Stanford University and Concordia University have also shown that bitcoin exchanges and other entities can prove assets, liabilities, and solvency without revealing their addresses using zero-knowledge proofs.[84]

According to Dan Blystone, “Ultimately, bitcoin resembles cash as much as it does credit cards.”[85]

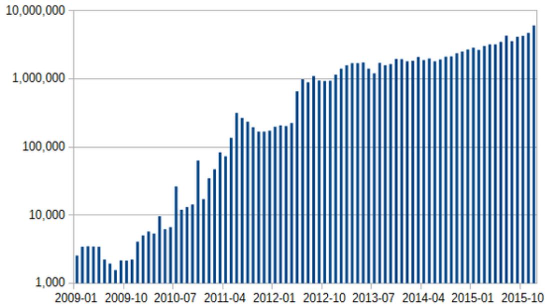
Fungibility

Wallets and similar software technically handle all bitcoins as equivalent, establishing the basic level of fungibility. Researchers have pointed out that the history of each bitcoin is registered and publicly available in the blockchain ledger, and that some users may refuse to accept bitcoins coming from controversial transactions, which would harm bitcoin’s fungibility.[86] Projects such as Zerocoin and Dark Wallet aim to address these privacy and fungibility issues.[87][88]

1.1.3 History

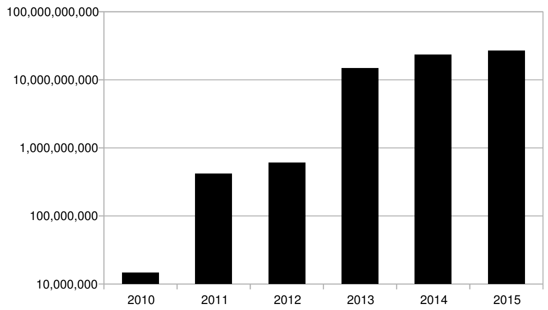
Main article: History of bitcoin

Bitcoin was invented by Satoshi Nakamoto,[13] who published the invention on 31 October 2008[14] in a research paper called “Bitcoin: A Peer-to-Peer Electronic Cash System”.[37] It was implemented as open source code and released in January 2009. Bitcoin is often called the first cryptocurrency[17][18][19] although prior systems existed.[note 5] Bitcoin is more correctly described as the first decentralized digital currency.[11][23]



Number of bitcoin transactions per month (logarithmic scale).[47]

One of the first supporters, adopters, contributor to bitcoin and receiver of the first bitcoin transaction was programmer Hal Finney. Finney downloaded the bitcoin software the day it was released, and received 10 bitcoins from Nakamoto in the world’s first bitcoin transaction.[89][90]



Liquidity (estimated, USD/year, logarithmic scale).[47]

Bitcoin’s 'shadowy inventor' Satoshi Nakamoto, is estimated to have mined 1 million bitcoins in the currency’s early days.[91]

Other early supporters were Wei Dai, creator of bitcoin predecessor *b-money*, and Nick Szabo, creator of bitcoin predecessor *bit gold*.[92]

Based on bitcoin’s open source code, other cryptocurrencies started to emerge in 2011.[24]

In March 2013, a technical glitch caused a fork in the blockchain, with one half of the network adding blocks to one version of the chain and the other half adding to another. For six hours two bitcoin networks operated at the same time, each with its own version of the transaction history. The core developers called for a temporary halt to transactions, sparking a sharp sell-off.[93] Normal operation was restored when the majority of the network downgraded to version 0.7 of the bitcoin software.[93]

In 2013 some mainstream websites began accepting bitcoins. WordPress had started in November 2012,[94] followed by OKCupid in April 2013,[95] TigerDirect[96] and Overstock.com in January 2014,[97] Expedia in June 2014,[98] Newegg and Dell in July 2014,[99] and Microsoft in December 2014.[100][note 9] The Electronic Frontier Foundation, a non-profit group, started accepting bitcoins in January 2011,[102] stopped accepting them in June 2011,[103] and began again in May 2013.[104]

In May 2013, the Department of Homeland Security seized assets belonging to the Mt. Gox exchange.[105] The U.S. Federal Bureau of Investigation (FBI) shut down the Silk Road website in October 2013.[106]

In October 2013, Chinese internet giant Baidu had allowed clients of website security services to pay with bitcoins.[107] During November 2013, the China-based bitcoin exchange BTC China overtook the Japan-based Mt. Gox and the Europe-based Bitstamp to become the largest bitcoin trading exchange by trade volume.[108] On 19 November 2013, the value of a bitcoin on the Mt. Gox exchange soared to a peak of US$900 after a United States Senate committee hearing was told by the FBI that virtual currencies are a legitimate financial service.[109]

On the same day, one bitcoin traded for over RMB¥6780 (US$1,100) in China.[110] On 5 December 2013, the People's Bank of China prohibited Chinese financial institutions from using bitcoins.[111] After the announcement, the value of bitcoins dropped,[112] and Baidu no longer accepted bitcoins for certain services.[113] Buying real-world goods with any virtual currency has been illegal in China since at least 2009.[114]

The first bitcoin ATM was installed in October 2013 in Vancouver, British Columbia, Canada.[115]

With about 12 million existing bitcoins in November 2013,[116] the new price increased the market cap for bitcoin to at least US$7.2 billion.[117] By 23 November 2013, the total market capitalization of bitcoin exceeded US$10 billion for the first time.[118]

In the U.S., two men were arrested in January 2014 on charges of money-laundering using bitcoins; one was Charlie Shrem, the head of now defunct bitcoin exchange BitInstant and a vice chairman of the Bitcoin Foundation. Shrem allegedly allowed the other arrested party to purchase large quantities of bitcoins for use on black-market websites.[119]

In early February 2014, one of the largest bitcoin exchanges, Mt. Gox,[74] suspended withdrawals citing technical issues.[120] By the end of the month, Mt. Gox had filed for bankruptcy protection in Japan amid reports that 744,000 bitcoins had been stolen.[121] Months before the filing, the popularity of Mt. Gox had waned as users experienced difficulties withdrawing funds.[122]

On 18 June 2014, it was announced that bitcoin payment service provider BitPay would become the new sponsor of St. Petersburg Bowl under a two-year deal, renamed the Bitcoin St. Petersburg Bowl. Bitcoin was to be accepted for ticket and concession sales at the game as part of the sponsorship, and the sponsorship itself was also paid for using bitcoin.[123]

Less than one year after the collapse of Mt. Gox, United Kingdom-based exhange Bitstamp announced that their exchange would be taken offline while they investigate a hack which resulted in about 19,000 bitcoins (equivalent to roughly US$5 million at that time) being stolen from their hot wallet.[124] The exchange remained offline for several days amid speculation that customers had lost their funds. Bitstamp resumed trading on 9 January after increasing security measures and assuring customers that their account balances would not be impacted.[125]

The bitcoin exchange service Coinbase launched the first regulated bitcoin exchange in 25 US states on 26 January 2015. At the time of the announcement, CEO Brian Armstrong stated that Coinbase intends to expand to thirty countries by the end of 2015.[126] A spokesperson for Benjamin M. Lawsky, the superintendent of New York state's Department of Financial Services, stated that Coinbase is operating without a license in the state of New York. Lawsky is responsible for the development of the so-called 'BitLicense', which companies need to acquire in order to legally operate in New York.[127]

In August 2015 it was announced that Barclays would become the first UK high street bank to start accepting bitcoin, with the bank revealing that it plans to allow users to make charitable donations using the currency.[128]

A major bitcoin exchange, Bitfinex, was hacked and nearly 120,000 BTC (around $60m) was stolen in 2016.[129]

1.1.4 Economics

Classification

According to the director of the Institute for Money, Technology and Financial Inclusion at the University of California-Irvine there is "an unsettled debate about whether bitcoin is a currency".[130] Bitcoin is commonly referred to with terms like: digital currency,[11]:1 digital cash,[131] virtual currency,[4] electronic currency,[38] or cryptocurrency.[130] Its inventor, Satoshi Nakamoto, used the term electronic cash.[37] Bitcoins have three useful qualities in a currency, according to the *Economist* in January 2015: they are "hard to earn, limited in supply and easy to verify".[60] Economists define money as a store of value, a medium of exchange, and a unit of account and agree that bitcoin has some way to go to meet all these criteria.[132] It does best as a medium of exchange, as of February 2015 the number of merchants accepting bitcoin has passed 100,000.[28] As of March 2014, the bitcoin market suffered from volatility, limiting the ability of bitcoin to act as a stable store of value, and retailers accepting bitcoin use other currencies as their principal unit of account.[132]

Journalists and academics also debate what to call bitcoin. Some media outlets do make a distinction between "real" money and bitcoins,[133] while others call bitcoin real money.[134] *The Wall Street Journal* declared it a commodity in December 2013.[135] A *Forbes* journalist referred to it as digital collectible.[136] Two University of Amsterdam computer scientists proposed the term "money-like informational commodity".[137] *The Wall Street Journal*,[138] *Wired*,[139] *Daily Mail Australia*,[140] *Forbes*,[10] *Business Wire*[141] and *Reuters*[142] used the digital asset classification for bitcoin. In a 2016 *Forbes* article, bitcoin was characterized as a member of a new asset class.[143]

The People's Bank of China has stated that bitcoin "is fundamentally not a currency but an investment target".[144]

In addition to the above, bitcoin is also characterized as a payment system.[11]:1

A Bitcoin ATM in California.

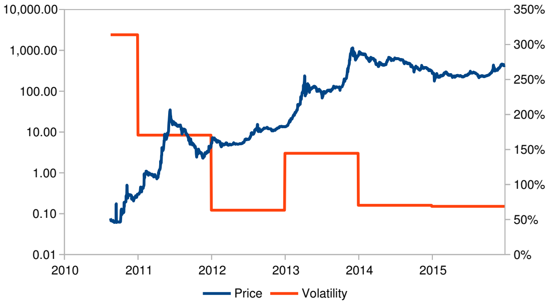
Buying and selling

Bitcoins can be bought and sold both on- and offline. Participants in online exchanges offer bitcoin buy and sell bids. Using an online exchange to obtain bitcoins entails some risk, and, according to a study published in April 2013, 45% of exchanges fail and take client bitcoins with them.[145] Exchanges have since implemented measures to provide proof of reserves in an effort to convey transparency to users.[146][147] Offline, bitcoins may be purchased directly from an individual[148] or at a bitcoin ATM.[149] Bitcoin machines are not however traditional ATMs. Bitcoin kiosks are machines connected to the Internet, allowing the insertion of cash in exchange for bitcoins. Bitcoin kiosks do not connect to a bank and may also charge transaction fees as high as 7% and exchange rates $50 over rates from elsewhere.[150]

Price and volatility

According to Mark T. Williams, as of 2014, bitcoin has volatility seven times greater than gold, eight times greater than the S&P 500, and eighteen times greater than the U.S. dollar.[151]

Attempting to explain the high volatility, a group of Japanese scholars stated that there is no stabilization mechanism.[152] The Bitcoin Foundation contends that high volatility is due to insufficient liquidity,[153] while a *Forbes* journalist claims that it is related to the uncertainty of its long-term value,[154] and the high volatility of a startup currency makes sense, “because people are still experimenting with the currency to figure out how useful it is.”[155]



Price[note 10] (left vertical axis, logarithmic scale) and volatility[note 11] (right vertical axis).[47]

There are uses where volatility does not matter, such as online gambling, tipping, and international remittances.[155] As of 2014, pro-bitcoin venture capitalists argued that the greatly increased trading volume that planned high-frequency trading exchanges would generate is needed to decrease price volatility.[156]

The price of bitcoins has gone through various cycles of appreciation and depreciation referred to by some as bubbles and busts.[157][158] In 2011, the value of one bitcoin rapidly rose from about US$0.30 to US$32 before returning to US$2.[159] In the latter half of 2012 and during the 2012–13 Cypriot financial crisis, the bitcoin price began to rise,[160] reaching a high of US$266 on 10 April 2013, before crashing to around US$50.[161] On 29 November 2013, the cost of one bitcoin rose to the all-time peak of US$1,242.[162] In 2014, the price fell sharply, and as of April remained depressed at little more than half 2013 prices. As of August 2014 it was under US$600.[163] In January 2015, noting that the bitcoin price had dropped to its lowest level since spring 2013 – around US$224 – *The New York Times* suggested that "[w]ith no signs of a rally in the offing, the industry is bracing for the effects of a prolonged decline in prices. In particular, bitcoin mining companies, which are essential to the currency’s underlying technology, are flashing warning signs.”[164] Also in January 2015, *Business Insider* reported that deep web drug dealers were “freaking out” as they lost profits through being unable to convert bitcoin revenue to cash quickly enough as the price declined – and that there was a danger that dealers selling reserves to stay in business might force the bitcoin price down further.[165]

On 4 November 2015, bitcoin had risen by more than 20%, exceeding $490. The *Financial Times* associated the rapid growth with the popularity of “socio-financial networks” MMM operated by Russian businessman Sergei Mavrodi.[166]

According to *The Wall Street Journal*, as of April 2016, bitcoin is starting to look slightly more stable than gold.[167]

Speculative bubble dispute

Bitcoin has been labelled a *speculative bubble* by many including former Fed Chairman Alan Greenspan[168] and economist John Quiggin.[169] Nobel Memorial Prize laureate Robert Shiller said that bitcoin "exhibited many of the characteristics of a speculative bubble".[170] Two lead software developers of bitcoin, Gavin Andresen[171] and Mike Hearn,[172] have warned that bubbles may occur. David Andolfatto, a vice president at the Federal Reserve Bank of St. Louis, stated, "Is bitcoin a bubble? Yes, if bubble is defined as a liquidity premium." According to Andolfatto, the price of bitcoin "consists purely of a bubble," but he concedes that many assets have prices that are greater than their intrinsic value.[48]:21 Journalist Matthew Boesler rejects the speculative bubble label and sees bitcoin's quick rise in price as nothing more than normal economic forces at work.[173] The *Washington Post* pointed out that the observed cycles of appreciation and depreciation don't correspond to the definition of speculative bubble.[159]

Ponzi scheme concerns

Various journalists, economists,[174][175] and bankers[176] have voiced concerns that bitcoin is a Ponzi scheme.[177] Eric Posner, a law professor at the University of Chicago, stated in 2013 that "a real Ponzi scheme takes fraud; bitcoin, by contrast, seems more like a collective delusion."[178] In 2014 reports by both the World Bank and the Swiss Federal Council examined the concerns and came to the conclusion that bitcoin is not a Ponzi scheme.[179]:7[180]:21

Value forecasts

Financial journalists and analysts, economists, and investors have attempted to predict the possible future value of bitcoin. In April 2013, economist John Quiggin stated, "bitcoins will attain their true value of zero sooner or later, but it is impossible to say when".[169] A similar forecast was made in November 2014 by economist Kevin Dowd.[181] In November 2014, David Yermack, Professor of Finance at New York University Stern School of Business, forecast that in November 2015 bitcoin may be all but worthless.[182] In the indicated period bitcoin has exchanged as low as $176.50 (January 2015) and during November 2015 the bitcoin low was $309.90.[47] In December 2013, finance professor Mark T. Williams forecast a bitcoin would be worth less than $10 by July 2014.[183] In the indicated period bitcoin has exchanged as low as $344 (April 2014) and during July 2014 the bitcoin low was $609.[47][184] In December 2014, Williams said, "The probability of success is low, but if it does hit, the reward will be very large."[185] In May 2013, Bank of America FX and Rate Strategist David Woo forecast a maximum fair value per bitcoin of $1,300.[186] Bitcoin investor Cameron Winklevoss stated in December 2013 that the "small bull case scenario for bitcoin is... 40,000 USD a coin".[187]

Obituaries

The "death" of bitcoin has been proclaimed numerous times.[188] One journalist has recorded 29 such "obituaries" as of early 2015.[188] *Forbes* magazine declared bitcoin "dead" in June 2011,[189] followed by *Gizmodo Australia* in August 2011.[190] *Wired* magazine wrote it had "expired" in December 2012.[191] *Ouishare Magazine* declared, "game over, bitcoin" in May 2013,[192] and *New York Magazine* stated bitcoin was "on its path to grave" in June 2013.[193] *Reuters* published an "obituary" for bitcoin in January 2014.[194] *Street Insider* declared bitcoin "dead" in February 2014,[195] followed by *The Weekly Standard* in March 2014,[196] *Salon* in March 2014,[197] *Vice News* in March 2014,[198] and *Financial Times* in September 2014.[199] In January 2015, *USA Today* states bitcoin was "headed to the ash heap",[200] and *The Telegraph* declared "the end of bitcoin experiment".[201] In January 2016, former bitcoin developer Mike Hearn called bitcoin a "failed project".[202] Peter Greenhill, Director of E-Business Development for the Isle of Man, commenting on the obituaries paraphrased Mark Twain saying "reports of bitcoin's death have been greatly exaggerated".[203]

Reception

Some economists have responded positively to bitcoin while others have expressed skepticism. François R. Velde, Senior Economist at the Chicago Fed described it as "an elegant solution to the problem of creating a digital currency".[204] Paul Krugman and Brad DeLong have found fault with bitcoin questioning why it should act as a reasonably stable store of value or whether there is a floor on its value.[205] Economist John Quiggin has criticized bitcoin as "the final refutation of the efficient-market hypothesis".[169]

David Andolfatto, Vice President at the Federal Reserve Bank of St. Louis, stated that bitcoin is a threat to the establishment, which he argues is a good thing for the Federal Reserve System and other central banks because it prompts these institutions to operate sound policies.[48]:33[206][207]

Free software movement activist Richard Stallman has criticized the lack of anonymity and called for reformed development.[208] PayPal President David A. Marcus calls bitcoin a "great place to put assets" but claims it will not be a currency until price volatility is reduced.[209] Bill Gates, in relation to the cost of moving money from place to place in an interview for Bloomberg L.P. stated: “Bitcoin is exciting because it shows how cheap it can be.”[210]

Officials in countries such as Brazil,[211] the Isle of Man,[212] Jersey,[213] the United Kingdom,[214] and the United States[33] have recognized its ability to provide legitimate financial services. Recent bitcoin developments have been drawing the interest of more financially savvy politicians and legislators as a result of bitcoin’s capability to eradicate fraud, simplify transactions, and provide transparency, when bitcoins are properly utilized.[215][216][217]

Acceptance by merchants

Bitcoins are accepted in this café in Delft in the Netherlands as of 2013

In 2015, the number of merchants accepting bitcoin exceeded 100,000.[28] Instead of 2–3% typically imposed by credit card processors, merchants accepting bitcoins often pay fees in the range from 0% to less than 2%.[29] As of December 2014 select firms that accept payments in bitcoin include:[note 9][note 12]

Acceptance by nonprofits

The Electronic Frontier Foundation,[104] Greenpeace,[245] The Mozilla Foundation,[246] and The Wikimedia Foundation.[247] Some U.S. political candidates, including New York City Democratic Congressional candidate Jeff Kurzon have said they would accept campaign donations in bitcoin.[248] In late 2013 the University of Nicosia became the first university in the world to accept bitcoins.[249]

Use in retail transactions

Due to the design of bitcoin, all retail figures are only estimates.[30][250] According to Tim Swanson, head of business development at a Hong Kong-based cryptocurrency technology company, in 2014, daily retail purchases made with bitcoin were worth about $2.3 million.[250] He estimates that, as of February 2015, fewer than 5,000 bitcoins per day (worth roughly $1.2 million at the time) were being used for retail transactions,[30] and concluded that in 2014 “it appears there has been very little if any increase in retail purchases using bitcoin.”[30]

bitcoin
ATM
KAUFEN SIE BITCOINS!
Berühren Sie den Bildschirm, um zu beginnen
Touch the screen to start
tipp3

A Bitcoin ATM in Vienna – Westbahnhof

Financial institutions

Bitcoin companies have had difficulty opening traditional bank accounts because lenders have been leery of bitcoin’s links to illicit activity.[251] According to Antonio Gallippi, a co-founder of BitPay, “banks are scared to deal with bitcoin companies, even if they really want to”.[252] In 2014, the National Australia Bank closed accounts of businesses with ties to bitcoin,[253] and HSBC refused to serve a hedge fund with links to bitcoin.[254] Australian banks in general have been reported as closing down bank accounts of operators of businesses involving the currency;[255] this has become the subject of an investigation by the Australian Competition and Consumer Commission.[255] Nonetheless, Australian banks have keenly adopted the blockchain technology on which

Bitcoin ATM in The D Las Vegas Casino. An early retail adopter of bitcoin

bitcoin is based.[256]

In a 2013 report, Bank of America Merrill Lynch stated that “we believe bitcoin can become a major means of payment for e-commerce and may emerge as a serious competitor to traditional money-transfer providers.”[257]

In June 2014, the first bank that converts deposits in currencies instantly to bitcoin without any fees was opened in Boston.[258]

As an investment

Some Argentinians have bought bitcoins to protect their savings against high inflation or the possibility that governments could confiscate savings accounts.[80] During the 2012–2013 Cypriot financial crisis, bitcoin purchases in Cyprus rose due to fears that savings accounts would be confiscated or taxed.[259] Other methods of investment are bitcoin funds. The first regulated bitcoin fund was established in Jersey in July 2014 and approved by the Jersey Financial Services Commission.[260] Also, c. 2012 an attempt was made by the Winklevoss twins (who in April 2013 claimed they owned nearly 1% of all bitcoins in existence[261]) to establish a bitcoin ETF.[262] As of early 2015, they have announced plans to launch a New York-based bitcoin exchange named Gemini,[263] which has received approval to launch on 5 October 2015.[264] On 4 May 2015, Bitcoin Investment Trust started trading on the OTCQX market as GBTC.[265] Forbes started publishing arguments in favor of investing in December 2015.[266]

In 2013 and 2014, the European Banking Authority[31] and the Financial Industry Regulatory Authority (FINRA), a United States self-regulatory organization,[267] warned that investing in bitcoins carries significant risks. Forbes named bitcoin the best investment of 2013.[268] In 2014, Bloomberg named bitcoin one of its worst investments of the year.[269] In 2015, bitcoin topped Bloomberg’s currency tables.[270]

To improve access to price information and increase transparency, on 30 April 2014 Bloomberg LP announced plans to list prices from bitcoin companies Kraken and Coinbase on its 320,000 subscription financial data terminals.[156][271] In May 2015, Intercontinental Exchange Inc., parent company of the New York Stock Exchange, announced a bitcoin index initially based on data from Coinbase transactions.[272]

Venture capital

Venture capitalists, such as Peter Thiel's Founders Fund, which invested US$3 million in BitPay, do not purchase bitcoins themselves, instead funding bitcoin infrastructure like companies that provide payment systems to merchants, exchanges, wallet services, etc.[273] In 2012, an incubator for bitcoin-focused start-ups was founded by Adam Draper, with financing help from his father, venture capitalist Tim Draper, one of the largest bitcoin holders after winning an auction of 30,000 bitcoins,[274] at the time called 'mystery buyer'.[275] The company’s goal is to fund 100 bitcoin businesses within 2–3 years with $10,000 to $20,000 for a 6% stake.[274] Investors also invest in bitcoin mining.[276] According to a 2015 study by Paolo Tasca, bitcoin startups raised almost $1 billion in three years (Q1 2012 – Q1 2015).[277]

Political economy

The decentralization of money offered by virtual currencies like bitcoin has its theoretical roots in the Austrian school of economics,[278] especially with Friedrich von Hayek in his book *Denationalisation of Money: The Argument Refined*, in which he advocates a complete free market in the production, distribution and management of money to end the monopoly of central banks.[279]

Bitcoin appeals to tech-savvy libertarians, because it so far exists outside the institutional banking system and the control of governments.[280] However, researchers looking to uncover the reasons for interest in bitcoin did not find evidence in Google search data that this was linked to libertarianism.[281]

Bitcoin's appeal reaches from left wing critics, "who perceive the state and banking sector as representing the same elite interests, [. . .] recognising in it the potential for collective direct democratic governance of currency"[282] and socialists proposing their "own states, complete with currencies",[283] to right wing critics suspicious of big government, at a time when activities within the regulated banking system were responsible for the severity of the financial crisis of 2007–08,[284] "because governments are not fully living up to the responsibility that comes with state-sponsored money".[285] Bitcoin has been described as "remov[ing] the imbalance between the big boys of finance and the disenfranchised little man, potentially allowing early adopters to negotiate favourable rates on exchanges and transfers – something that only the very biggest firms have traditionally enjoyed".[286] Two WSJ journalists describe bitcoin in their book as "about freeing people from the tyranny of centralised trust".[287]

1.1.5 Legal status and regulation

Main article: Legality of bitcoin by country

The legal status of bitcoin varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed its use and trade, others have banned or restricted it. Likewise, various government agencies, departments, and courts have classified bitcoins differently. Regulations and bans that apply to bitcoin probably extend to similar cryptocurrency systems.[288]

In April 2013, Steven Strauss, a Harvard public policy professor, suggested that governments could outlaw bitcoin,[289] and this possibility was mentioned again by a bitcoin investment vehicle in a July 2013 report to a regulator.[262] However, the vast majority of nations have not done so as of 2014. It is illegal in Bangladesh,[290] Bolivia,[291] Ecuador.[292]

In China in December 2013 the Chinese government declared that "bitcoin is not a currency and should not be circulated and used in the market as a currency." 'While people there are free to buy and sell it, financial institutions have been warned away'.[293]

1.1.6 Criminal activity

The use of bitcoin by criminals has attracted the attention of financial regulators, legislative bodies, law enforcement, and the media.[32] The FBI prepared an intelligence assessment,[34] the SEC has issued a pointed warning about investment schemes using virtual currencies,[32] and the U.S. Senate held a hearing on virtual currencies in November 2013.[33]

Several news outlets have asserted that the popularity of bitcoins hinges on the ability to use them to purchase illegal goods.[294][295] In 2014, researchers at the University of Kentucky found "robust evidence that computer programming enthusiasts and illegal activity drive interest in bitcoin, and find limited or no support for political and investment motives."[281]

Theft

There have been many cases of bitcoin theft.[68] One way this is accomplished involves a third party accessing the private key to a victim's bitcoin address,[296] or of an online wallet.[297] If the private key is stolen, all the bitcoins from the compromised address can be transferred. In that case, the network does not have any provisions to identify the thief, block further transactions of those stolen bitcoins, or return them to the legitimate owner.[262]

Theft also occurs at sites where bitcoins are used to purchase illicit goods. In late November 2013, an estimated $100 million in bitcoins were allegedly stolen from the online illicit goods marketplace Sheep Marketplace, which immediately closed.[298] Users tracked the coins as they were processed and converted to cash, but no funds were recovered and no culprits identified.[298] A different black market, Silk Road 2, stated that during a February 2014 hack, bitcoins valued at $2.7 million were taken from escrow accounts.[299]

Sites where users exchange bitcoins for cash or store them in "wallets" are also targets for theft. Inputs.io, an Australian wallet service, was hacked twice in October 2013 and lost more than $1 million in bitcoins.[300] In late February 2014 Mt. Gox, one of the largest virtual currency exchanges, filed for bankruptcy in Tokyo amid reports that bitcoins worth $350 million had been stolen.[121] Flexcoin, a bitcoin storage specialist based in Alberta, Canada, shut down on March 2014 after saying it discovered a theft of about $650,000 in bitcoins.[301] Poloniex, a digital currency exchange, reported on March 2014 that it lost bitcoins valued at around $50,000.[302] In January 2015 UK-based bitstamp, the third busiest bitcoin exchange globally, was hacked and $5 million in bitcoins were stolen.[303] February 2015 saw a Chinese exchange named BTER lose bitcoins worth nearly $2 million to hackers.[304]

A major bitcoin exchange, Bitfinex, was hacked and nearly 120,000 bitcoins (around $60m) was stolen in 2016. Bitfinex was forced to suspend its trading. The theft is the second largest bitcoin heist ever, dwarfed only by Mt. Gox theft in 2014. According to *Forbes*, "All of Bitfinex's customers,... will stand to lose money. The company has announced a haircut of 36.067% across the board."[129]

Black markets

Main article: Darknet market

A CMU researcher estimated that in 2012, 4.5% to 9% of all transactions on all exchanges in the world were for drug trades on a single deep web drugs market, Silk Road.[305] Child pornography,[306] murder-for-hire services,[307] and weapons[308] are also allegedly available on black market sites that sell in bitcoin. Due to the anonymous nature and the lack of central control on these markets, it is hard to know whether the services are real or just trying to take the bitcoins.[309]

Several deep web black markets have been shut by authorities. In October 2013 Silk Road was shut down by U.S. law enforcement[310][311][312] leading to a short-term decrease in the value of bitcoin.[313] In 2015, the founder of the site was sentenced to life in prison.[314] Alternative sites were soon available, and in early 2014 the Australian Broadcasting Corporation reported that the closure of Silk Road had little impact on the number of Australians selling drugs online, which had actually increased.[315] In early 2014, Dutch authorities closed Utopia, an online illegal goods market, and seized 900 bitcoins.[316] In late 2014, a joint police operation saw European and American authorities seize bitcoins and close 400 deep web sites including the illicit goods market Silk Road 2.0.[317] Law enforcement activity has resulted in several convictions. In December 2014, Charlie Shrem was sentenced to two years in prison for indirectly helping to send $1 million to the Silk Road drugs site,[318] and in February 2015, its founder, Ross Ulbricht, was convicted on drugs charges and faces a life sentence.[319]

Some black market sites may seek to steal bitcoins from customers. The bitcoin community branded one site, Sheep Marketplace, as a scam when it prevented withdrawals and shut down after an alleged bitcoins theft.[320] In a separate case, escrow accounts with bitcoins belonging to patrons of a different black market were hacked in early 2014.[299]

According to the Internet Watch Foundation, a UK-based charity, bitcoin is used to purchase child pornography, and almost 200 such websites accept it as payment. Bitcoin isn't the sole way to purchase child pornography online, as Troels Oertling, head of the cybercrime unit at Europol, states, “Ukash and Paysafecard... have [also] been used to pay for such material.” However, the Internet Watch Foundation lists around 30 sites that exclusively accept bitcoins.[306] Some of these sites have shut down, such as a deep web crowdfunding website that aimed to fund the creation of new child porn.[321] Furthermore, hyperlinks to child porn websites have been added to the blockchain as arbitrary data can be included when a transaction is made.[322][323]

Money laundering

Bitcoins may not be ideal for money laundering because all transactions are public.[324] Authorities, including the European Banking Authority[31] the FBI,[34] and the Financial Action Task Force of the G7[325] have expressed concerns that bitcoin may be used for money laundering. In early 2014, an operator of a U.S. bitcoin exchange was arrested for money laundering.[119] A report by UK’s Treasury and Home Office named “UK national risk assessment of money laundering and terrorist financing” (2015 October) found that, of the twelve methods examined in the report, bitcoin carries the lowest risk of being used for money laundering, with the most common money laundering method being the banks.[326]

Ponzi scheme

In a Ponzi scheme that utilized bitcoins, The Bitcoin Savings and Trust promised investors up to 7 percent weekly interest, and raised at least 700,000 bitcoins from 2011 to 2012.[327] In July 2013 the U.S. Securities and Exchange Commission charged the company and its founder in 2013 “with defrauding investors in a Ponzi scheme involving bitcoin”.[327] In September 2014 the judge fined Bitcoin Savings & Trust and its owner $40 million for operating a bitcoin Ponzi scheme.[328]

Malware

Bitcoin-related malware includes software that steals bitcoins from users using a variety of techniques, software that uses infected computers to mine bitcoins, and different types of ransomware, which disable computers or prevent files from being accessed until some payment is made. Security company Dell SecureWorks said in February 2014 that it had identified almost 150 types of bitcoin malware.[329]

Unauthorized mining In June 2011, Symantec warned about the possibility that botnets could mine covertly for bitcoins.[330] Malware used the parallel processing capabilities of GPUs built into many modern video cards.[331] Although the average PC with an integrated graphics processor is virtually useless for bitcoin mining, tens of thousands of PCs laden with mining malware could produce some results.[332]

In mid-August 2011, bitcoin mining botnets were detected,[333] and less than three months later, bitcoin mining trojans had infected Mac OS X.[334]

In April 2013, electronic sports organization E-Sports Entertainment was accused of hijacking 14,000 computers to mine bitcoins; the company later settled the case with the State of New Jersey.[335]

German police arrested two people in December 2013 who customized existing botnet software to perform bitcoin mining, which police said had been used to mine at least $950,000 worth of bitcoins.[336]

For four days in December 2013 and January 2014, Yahoo! Europe hosted an ad containing bitcoin mining malware that infected an estimated two million computers.[337] The software, called Sefnit, was first detected in mid-2013 and has been bundled with many software packages. Microsoft has been removing the malware through its Microsoft Security Essentials and other security software.[338]

Several reports of employees or students using university or research computers to mine bitcoins have been published.[339]

Malware stealing Some malware can steal private keys for bitcoin wallets allowing the bitcoins themselves to be stolen. The most common type searches computers for cryptocurrency wallets to upload to a remote server where they can be cracked and their coins stolen.[340] Many of these also log keystrokes to record passwords, often avoiding the need to crack the keys.[340] A different approach detects when a bitcoin address is copied to a clipboard and quickly replaces it with a different address, tricking people into sending bitcoins to the wrong address.[341] This method is effective because bitcoin transactions are irreversible.

One virus, spread through the Pony botnet, was reported in February 2014 to have stolen up to $220,000 in cryptocurrencies including bitcoins from 85 wallets.[342] Security company Trustwave, which tracked the malware, reports that its latest version was able to steal 30 types of digital currency.[343]

A type of Mac malware active in August 2013, Bitvanity posed as a vanity wallet address generator and stole addresses and private keys from other bitcoin client software.[344] A different trojan for Mac OS X, called CoinThief was reported in February 2014 to be responsible for multiple bitcoin thefts.[344] The software was hidden in versions of some cryptocurrency apps on Download.com and MacUpdate.[344]

Ransomware Another type of bitcoin-related malware is ransomware. One program called CryptoLocker, typically spread through legitimate-looking email attachments, encrypts the hard drive of an infected computer, then displays a countdown timer and demands a ransom, usually two bitcoins, to decrypt it.[345] Massachusetts police said they paid a 2 bitcoin ransom in November 2013, worth more than $1,300 at the time, to decrypt one of their hard drives.[346] Linkup, a combination ransomware and bitcoin mining program that surfaced in February 2014, disables internet access and demands credit card information to restore it, while secretly mining bitcoins.[345]

1.1.7 Security

Various potential attacks on the bitcoin network and its use as a payment system, real or theoretical, have been considered. The bitcoin protocol includes several features that protect it against some of those attacks, such as unauthorized spending, double spending, forging bitcoins, and tampering with the blockchain. Other attacks, such as theft of private keys, require due care by users.[11][347][348][349][2][350][351]

Unauthorized spending

Unauthorized spending is mitigated by bitcoin's implementation of public-private key cryptography. For example; when Alice sends a bitcoin to Bob, Bob becomes the new owner of the bitcoin. Eve observing the transaction might want to spend the bitcoin Bob just received, but she cannot sign the transaction without the knowledge of Bob's private key.[11]

Double spending

A specific problem that an internet payment system must solve is double-spending, whereby a user pays the same coin to two or more different recipients. An example of such a problem would be if Eve sent a bitcoin to Alice and later sent the same bitcoin to Bob. The bitcoin network guards against double-spending by recording all bitcoin transfers in a ledger (the blockchain) that is visible to all users, and ensuring for all transferred bitcoins that they haven't been previously spent.[11]:4

Race attack

If Eve offers to pay Alice a bitcoin in exchange for goods and signs a corresponding transaction, it is still possible that she also creates a different transaction at the same time sending the same bitcoin to Bob. By the rules, the network accepts only one of the transactions. This is called a race attack, since there is a race which transaction will be accepted first. Alice can reduce the risk of race attack stipulating that she will not deliver the goods until Eve's payment to Alice appears in the blockchain.[347]

A variant race attack (which has been called a Finney attack by reference to Hal Finney) requires the participation of a miner. Instead of sending both payment requests (to pay Bob and Alice with the same coins) to the network, Eve issues only Alice's payment request to the network, while the accomplice tries to mine a block that includes the payment to Bob instead of Alice. There is a positive probability that the rogue miner will succeed before the network, in which case the payment to Alice will be rejected. As with the plain race attack, Alice can reduce the risk of a Finney attack by waiting for the payment to be included in the blockchain.[348]

History modification

Each block that is added to the blockchain, starting with the block containing a given transaction, is called a confirmation of that transaction. Ideally, merchants and services that receive payment in bitcoin should wait for at least one confirmation to be distributed over the network, before assuming that the payment was done. The more confirmations that the merchant waits for, the more difficult it is for an attacker to successfully reverse the transaction in a blockchain—unless the attacker controls more than half the total network power, in which case it is called a 51% attack.[349]

Deanonymisation of clients

Along with transaction graph analysis, which may reveal connections between bitcoin addresses (pseudonyms),[2][350] there is a possible attack[351] which links a user's pseudonym to its IP address. If the peer is using Tor, the attack includes a method to separate the peer from the Tor network, forcing them to use their real IP address for any further transactions. The attack makes use of bitcoin mechanisms of relaying peer addresses and anti-DoS protection. The cost of the attack on the full bitcoin network is under €1500 per month.[351]

1.1.8 Data in the blockchain

While it is possible to store any digital file in the blockchain, the larger the transaction size, the larger any associated fees become.[352] Various items have been embedded, including URLs to child pornography, an ASCII art image of Ben Bernanke, material from the Wikileaks cables, prayers from bitcoin miners, and the original bitcoin whitepaper.[353]

1.1.9 In academia

In the fall of 2014, undergraduate students at the Massachusetts Institute of Technology (MIT) each received bitcoins worth $100 “to better understand this emerging technology”. The bitcoins were not provided by MIT but rather the MIT Bitcoin Club, a student-run club.[354][355]

1.1.10 In art, entertainment, and media

Films

A documentary film called *The Rise and Rise of Bitcoin* (late 2014) features interviews with people who use bitcoin, such as a computer programmer and a drug dealer.[356]

Music

Several lighthearted songs celebrating bitcoin have been released.[357]

Literature

In Charles Stross' science fiction novel *Neptune’s Brood* (2014), a modification of bitcoin is used as the universal interstellar payment system. The functioning of the system is a major plot element of the book.[358]

Television

In early 2015, the CNN series *Inside Man* featured an episode about bitcoin. Filmed in July 2014, it featured Morgan Spurlock living off of bitcoins for a week to figure out whether the world is ready for a new kind of money.[359]

1.1.11 See also

- Alternative currency
- Bitcoin Center NYC
- Bitcoin Classic
- Bitcoin XT
- Coinscrum
- Comparison of bitcoin wallets
- Crypto-anarchism
- Decentralized autonomous organization
- Digital gold currency
- Private currency
- World currency
- Comparison of payment systems

1.1.12 Notes

[1] Bitcoin does not have a central authority.[1]</ref>Date of introduction 3 January 2009User(s) WorldwideSupply growth 12.5 bitcoins per block (approximately every ten minutes) until mid 2020,[2] and then afterwards 6.25 bitcoins per block for 4 years until next halving. This halving continues until 2110–40, when 21 million bitcoins will have been issued.Subunit 10^{-3} millibitcoin 10^{-6} microbitcoin, bit[3] 10^{-8} satoshi[4]Symbol BTC,[note 2] It does not conform to ISO 4217 as BT is the country code of Bhutan.

[2] As of 2014, BTC is a commonly used code.<ref name='standardize'>Nermin Hajdarbegovic (7 October 2014). "Bitcoin Foundation to Standardise Bitcoin Symbol and Code Next Year". CoinDesk. Retrieved 28 January 2015.

[3] As of 2014, XBT, a code that conforms to ISO 4217 though is not officially part of it, is used by Bloomberg L.P.,[5] CNNMoney,[6] and xe.com.[7]

[4] The proposal for the addition of bitcoin sign ₿ has been accepted by Unicode.[8]</ref> Ƀ[9] millibitcoin mBTC microbitcoin, bit[3] µBTCCoins Unspent outputs of transactions denominated in any multiple of satoshis<ref name='Antonopoulos2014' group=''>

[5] DigiCash was first used for a transaction in 1994,[20][21] and OpenCoin, now known as Ripple, had code written prior to November 2008.[22]

[6] Relative mining difficulty is defined as the ratio of the difficulty target on 9 January 2009 to the current difficulty target.

[7] It is misleading to think that there is an analogy between gold mining and bitcoin mining. The fact is that gold miners are rewarded for producing gold, while bitcoin miners are not rewarded for producing bitcoins; they are rewarded for their record-keeping services.[48]

[8] The exact number is 20,999,999.9769 bitcoins.[43]:ch. 8

[9] Some of these firms use bitcoin payment processors such as BitPay and Coinbase and do not handle or store bitcoins themselves.[101]

[10] The price of 1 bitcoin in U.S. dollars.

[11] Volatility is calculated on a yearly basis.

[12] Retailers usually offer in-store credit, instead of a return transfer (or chargeback) as the only option when customers return items purchased with bitcoins.[218]

1.1.13 References

[1] "Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy". *fincen.gov*. Financial Crimes Enforcement Network. 19 November 2013. Retrieved 1 June 2014.

[2] Ron Dorit; Adi Shamir (2012). "Quantitative Analysis of the Full Bitcoin Transaction Graph" (PDF). Cryptology ePrint Archive. Retrieved 18 October 2012.

[3] Garzik, Jeff (2 May 2014). "BitPay, Bitcoin, and where to put that decimal point". Retrieved 20 November 2015.

[4] Jason Mick (12 June 2011). "Cracking the Bitcoin: Digging Into a $131M USD Virtual Currency". Daily Tech. Retrieved 30 September 2012.

[5] Romain Dillet (9 August 2013). "Bitcoin Ticker Available On Bloomberg Terminal For Employees". TechCrunch. Retrieved 2 November 2014.

[6] "Bitcoin Composite Quote (XBT)". *CNN Money*. CNN. Retrieved 2 November 2014.

[7] "XBT – Bitcoin". xe.com. Retrieved 2 November 2014.

[8] Shirriff, Ken (2 October 2015). "Proposal for addition of bitcoin sign" (PDF). *unicode.org*. Unicode. Retrieved 3 November 2015.

[9] Cawrey, Daniel (2014-04-09). "Industry group aims to change bitcoin symbol to 'Ƀ'". *CoinDesk*.

[10] Shin, Laura (21 October 2015). "Q&A: Chain.com CEO Adam Ludwin On How Money Will Become Digital". Forbes. Retrieved 4 January 2016.

[11] Jerry Brito & Andrea Castillo (2013). "Bitcoin: A Primer for Policymakers" (PDF). *Mercatus Center*. George Mason University. Retrieved 22 October 2013.

[12] http://www.dailyherald.com/article/20150613/business/150619551/ Retrieved September- 23-2016

[13] S., L. (2 November 2015). "Who is Satoshi Nakamoto?". *The Economist*. The Economist Newspaper Limited. Retrieved 23 September 2016.

[14] Vigna, Paul; Casey, Michael J. (January 2015). *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order* (1 ed.). New York: St. Martin's Press. ISBN 978-1-250-06563-6.

[15] Davis, Joshua (10 October 2011). "The Crypto-Currency: Bitcoin and its mysterious inventor". *The New Yorker*. Retrieved 31 October 2014.

[16] Joshua Kopstein (12 December 2013). "The Mission to Decentralize the Internet". The New Yorker. Retrieved 30 December 2014. The network's "nodes"—users running the bitcoin software on their computers—collectively check the integrity of other nodes to ensure that no one spends the same coins twice. All transactions are published on a shared public ledger, called the "blockchain"

[17] "Drug market moving quickly online, global user survey finds". *South China Morning Post*. South China Morning Post Publishers. 14 April 2014. Retrieved 7 January 2015.

[18] Sparkes, Matthew (9 June 2014). "The coming digital anarchy". *The Telegraph*. London: Telegraph Media Group Limited. Retrieved 7 January 2015.

[19] Lachance Shandrow, Kim (30 May 2014). "This Company Is Now the Largest in the World to Accept Bitcoin". *entrepreneur.com*. Entrepreneur Media, Inc. Retrieved 7 January 2015.

[20] "World's first electronic cash payment over computer networks.". Electronic Frontier Foundation. 26 May 1994. Retrieved 20 November 2015.

[21] Greenberg, Andy (2012). *This Machine Kills Secrets: How WikiLeakers, Hacktivists, and Cypherpunks Are Freeing the World's Information*. Ebury Publishing. ISBN 978-0-7535-4801-1.

[22] "OpenCoin/opencoin-historic". *github.com*. GitHub, Inc. Retrieved 8 May 2015.

[23] Sagona-Stophel, Katherine. "Bitcoin 101 white paper" (PDF). Thomson Reuters. Retrieved 20 November 2015.

[24] Espinoza, Javier (22 September 2014). "Is It Time to Invest in Bitcoin? Cryptocurrencies Are Highly Volatile, but Some Say They Are Worth It". *Journal Reports*. The Wall Street Journal. Retrieved 28 June 2016.

[25] "What is Bitcoin?". CNN Money. Retrieved 16 November 2015.

[26] Natasha Lomas (16 September 2013). "BitPay Passes 10,000 Bitcoin-Accepting Merchants On Its Payment Processing Network". *Techcrunch*. Techcrunch.com. Retrieved 21 October 2013.

[27] Joshua A. Kroll; Ian C. Davey; Edward W. Felten (11–12 June 2013). "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries" (PDF). *The Twelfth Workshop on the Economics of Information Security (WEIS 2013)*. Retrieved 26 April 2016. A transaction fee is like a tip or gratuity left for the miner.

[28] Cuthbertson, Anthony (4 February 2015). "Bitcoin now accepted by 100,000 merchants worldwide". *International Business Times*. IBTimes Co., Ltd. Retrieved 20 November 2015.

[29] Wingfield, Nick (30 October 2013). "Bitcoin Pursues the Mainstream". *The New York Times*. Retrieved 4 November 2013.

[30] Orcutt, Mike (18 February 2015). "Is Bitcoin Stalling?". *MIT Technology Review*. Retrieved 20 February 2015.

[31] "Warning to consumers on virtual currencies". European Banking Authority. 12 December 2013. Archived from the original (PDF) on 28 December 2013. Retrieved 23 December 2013.

[32] Lavin, Tim (8 August 2013). "The SEC Shows Why Bitcoin Is Doomed". *bloomberg.com*. Bloomberg LP. Retrieved 20 October 2013.

[33] Tracy, Ryan (18 November 2013). "Authorities See Worth of Bitcoin". *Markets*. The Wall Street Journal. Retrieved 28 November 2014.

[34] "Bitcoins Virtual Currency: Unique Features Present Challenges for Deterring Illicit Activity" (PDF). *Cyber Intelligence Section and Criminal Intelligence Section*. FBI. 24 April 2012. Retrieved 2 November 2014.

[35] Timothy B. Lee & Hayley Tsukayama (2 October 2013). "Authorities shut down Silk Road, the world's largest Bitcoin-based drug market". *The Washington Post*. Retrieved 21 October 2013.

[36] "bitcoin". Oxford University Press. Retrieved 28 December 2014.

[37] Nakamoto, Satoshi (October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). bitcoin.org. Retrieved 28 April 2014.

[38] Bustillos, Maria (2 April 2013). "The Bitcoin Boom". *The New Yorker*. Condé Nast. Retrieved 22 December 2013. Standards vary, but there seems to be a consensus forming around Bitcoin, capitalized, for the system, the software, and the network it runs on, and bitcoin, lowercase, for the currency itself.

[39] Vigna, Paul (3 March 2014). "BitBeat: Is It Bitcoin, or bitcoin? The Orthography of the Cryptography". *WSJ*. Retrieved 21 April 2014.

[40] Metcalf, Allan (14 April 2014). "The latest style". Lingua Franca blog. The Chronicle of Higher Education (chronicle.com). Retrieved 19 April 2014.

[41] "Blockchain". Investopedia. Retrieved 28 June 2016.

[42] "Bitcoin Wallet". Investopedia. Retrieved 28 June 2016.

[43] Andreas M. Antonopoulos (April 2014). *Mastering Bitcoin. Unlocking Digital Crypto-Currencies*. O'Reilly Media. ISBN 978-1-4493-7404-4.

[44] "Regulation of Bitcoin in Selected Jurisdictions" (PDF). The Law Library of Congress, Global Legal Research Center. January 2014. Retrieved 26 August 2014.

[45] Katie Pisa & Natasha Maguder (9 July 2014). "Bitcoin your way to a double espresso". *cnn.com*. CNN. Retrieved 23 April 2015.

[46] "Man Throws Away 7,500 Bitcoins, Now Worth $7.5 Million". *CBS DC*. 29 November 2013. Retrieved 23 January 2014.

[47] "Charts". Blockchain.info. Retrieved 2 November 2014.

[48] Andolfatto, David (31 March 2014). "Bitcoin and Beyond: The Possibilities and Pitfalls of Virtual Currencies" (PDF). *Dialogue with the Fed*. Federal Reserve Bank of St. Louis. Retrieved 16 April 2014.

[49] "The great chain of being sure about things". *The Economist*. The Economist Newspaper Limited. 31 October 2015. Retrieved 3 July 2016.

[50] "Difficulty History" (The ratio of all hashes over valid hashes is D x 4295032833, where D is the published "Difficulty" figure.). Blockchain.info. Retrieved 26 March 2015.

[51] Hampton, Nikolai (5 September 2016). "Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin". *Computerworld*. IDG. Retrieved 5 September 2016.

[52] Mills, Kelly (3 April 2014). "Bitcoins lose viability". *The Arbiter*. Boise State Student Media. Retrieved 14 April 2014.

[53] Wang, Luqin; Liu, Yong. "Exploring Miner Evolution in Bitcoin Network" (PDF). NYU Polytechnic School of Engineering. Retrieved 15 February 2015.

[54] Rosenfeld, Meni. "Analysis of Bitcoin Pooled Mining Reward Systems". arXiv:1112.4980.

[55] Peter Svensson (17 June 2014). "Bitcoin faces biggest threat yet: a miner takeover". Retrieved 8 January 2015.

[56] Rockman, Simon (17 January 2014). "Manic miners: Ten Bitcoin generating machines". The Register. Retrieved 13 February 2014.

[57] Bays, Jason (9 April 2014). "Bitcoin offers speedy currency, poses high risks". *Purdue Exponent*. The Exponent Online. Retrieved 14 April 2014.

[58] Gimein, Mark (13 April 2013). "Virtual Bitcoin Mining Is a Real-World Environmental Disaster". *Bloomberg Business*. Bloomberg LP. Retrieved 22 April 2015.

[59] O'Dwyer, Karl J.; Malone, David (26 June 2014). "Bitcoin Mining and its Energy Footprint" (PDF). *ISSC*. Hamilton Institute. Retrieved 18 September 2016.

[60] "The magic of mining". *The Economist*. 13 January 2015. Retrieved 13 January 2015.

[61] O'Brien, Matt (13 June 2015). "The scam called Bitcoin". *DailyHerald*. Retrieved 20 September 2016.

[62] Ashlee Vance (14 November 2013). "2014 Outlook: Bitcoin Mining Chips, a High-Tech Arms Race". Businessweek. Retrieved 24 November 2013.

[63] "Block #420000". Blockchain.info. Retrieved 11 September 2016.

[64] Ritchie S. King; Sam Williams; David Yanofsky (17 December 2013). "By reading this article, you're mining bitcoins". *qz.com*. Atlantic Media Co. Retrieved 17 December 2013.

[65] Shin, Laura (24 May 2016). Retrieved July-13-2016 "Bitcoin Production Will Drop By Half In July, How Will That Affect The Price?" Check |url= value (help). *Forbes*. Retrieved 13 July 2016.

[66] Adam Serwer & Dana Liebelson (10 April 2013). "Bitcoin, Explained". *motherjones.com*. Mother Jones. Retrieved 26 April 2014.

[67] Villasenor, John (26 April 2014). "Secure Bitcoin Storage: A Q&A With Three Bitcoin Company CEOs". *forbes.com*. Forbes. Retrieved 26 April 2014.

[68] "Bitcoin: Bitcoin under pressure". *The Economist*. 30 November 2013. Retrieved 30 November 2013.

[69] Skudnov, Rostislav (2012). *Bitcoin Clients* (PDF) (Bachelor's Thesis). Turku University of Applied Sciences. Retrieved 16 January 2014.

[70] "Blockchain Size". Blockchain.info. Retrieved 24 April 2016.

[71] Gervais, Arthur; O. Karame, Ghassan; Gruber, Damian; Capkun, Srdjan. "On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients" (PDF). Retrieved 3 September 2016.

[72] Jon Matonis (26 April 2012). "Be Your Own Bank: Bitcoin Wallet for Apple". Forbes. Retrieved 17 November 2014.

[73] Bill Barhydt (4 June 2014). "3 reasons Wall Street can't stay away from bitcoin". NBCUniversal. Retrieved 2 April 2015.

[74] "MtGox gives bankruptcy details". *bbc.com*. BBC. 4 March 2014. Retrieved 13 March 2014.

[75] Staff, Verge (13 December 2013). "Casascius, maker of shiny physical bitcoins, shut down by Treasury Department". The Verge. Retrieved 10 January 2014.

[76] Eric Mu (15 October 2014). "Meet Trezor, A Bitcoin Safe That Fits Into Your Pocket". *Forbes Asia*. Forbes. Retrieved 31 October 2014.

[77] "Bitcoin Core version 0.9.0 released". *bitcoin.org*. Retrieved 8 January 2015.

[78] Metz, Cade (19 August 2015). "The Bitcoin Schism Shows the Genius of Open Source". *Wired*. Condé Nast. Retrieved 3 July 2016.

[79] Simonite, Tom (5 September 2013). "Mapping the Bitcoin Economy Could Reveal Users' Identities". *MIT Technology Review*. Retrieved 2 April 2014.

[80] Lee, Timothy (21 August 2013). "Five surprising facts about Bitcoin". The Washington Post. Retrieved 2 April 2014.

[81] McMillan, Robert (6 June 2013). "How Bitcoin lets you spy on careless companies". *wired.co.uk*. Conde Nast. Retrieved 2 April 2014.

[82] Potts, Jake (31 July 2015). "Mastering Bitcoin Privacy". Airbitz. Retrieved 23 February 2016.

[83] Matonis, Jon (5 June 2013). "The Politics Of Bitcoin Mixing Services". *forbes.com*. Forbes. Retrieved 2 April 2014.

[84] Gaby G. Dagher, Benedikt Bünz, Joseph Bonneau, Jeremy Clark and Dan Boneh (26 October 2015). "Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges" (PDF). International Association for Cryptologic Research. Retrieved 23 February 2016.

[85] Blystone, Dan. "Bitcoin Transactions Vs. Credit Card Transactions". *Investopedia*. Retrieved 3 September 2016.

[86] Ben-Sasson, Eli; Chiesa, Alessandro; Garman, Christina; Green, Matthew; Miers, Ian; Tromer, Eran; Virza, Madars (2014). "Zerocash: Decentralized Anonymous Payments from Bitcoin" (PDF). *2014 IEEE Symposium on Security and Privacy*. IEEE computer society. Retrieved 31 October 2014.

[87] Miers, Ian; Garman, Christina; Green, Matthew; Rubin, Aviel. "Zerocoin: Anonymous Distributed E-Cash from Bitcoin" (PDF). Johns Hopkins University. Retrieved 15 February 2015.

[88] Greenberg, Andy (29 April 2014). "'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever". *Wired*. Retrieved 15 February 2015.

[89] Peterson, Andrea (3 January 2014). "Hal Finney received the first Bitcoin transaction. Here's how he describes it.". *The Washington Post*.

[90] Popper, Nathaniel (30 August 2014). "Hal Finney, Cryptographer and Bitcoin Pioneer, Dies at 58". *NYTimes*. Retrieved 2 September 2014.

[91] https://www.wired.com/2013/12/fbi_wallet/ Retrieved September-16-2016

[92] Wallace, Benjamin (23 November 2011). "The Rise and Fall of Bitcoin". *Wired*. Retrieved 4 November 2013.

[93] Lee, Timothy (11 March 2013). "Major glitch in Bitcoin network sparks sell-off; price temporarily falls 23%". arstechnica.com. Retrieved 15 February 2015.

[94] Skelton, Andy (15 November 2012). "Pay Another Way: Bitcoin". WordPress. Retrieved 24 April 2014.

[95] Franceschi-Bicchierai, Lorenzo (18 April 2013). "OKCupid Now Accepts Bitcoin". Mashable. Retrieved 24 April 2014.

[96] Jane McEntegart (26 January 2014). "TigerDirect is Now Accepting Bitcoin As Payment". Tom's hardware. Retrieved 28 August 2014.

[97] Vaishampayan, Saumya (9 January 2014). "Bitcoin now accepted on Overstock.com through VC-backed Coinbase". *marketwatch.com*. Wall Street Journal. Retrieved 10 February 2014.

[98] Biggs, John (11 June 2014). "Expedia Now Accepts Bitcoin For Your Crypto-Vacations". Techcrunch. Retrieved 12 June 2014.

[99] Flacy, Mike (19 July 2014). "Dell, Newegg Start Accepting Bitcoin as Payment". Digital Trends. Retrieved 5 August 2014.

[100] Tom Warren (11 December 2014). "Microsoft now accepts Bitcoin to buy Xbox games and Windows apps". *The Verge*. Vox Media. Retrieved 11 December 2014.

[101] Chavez-Dreyfuss, Gertrude; Connor, Michael (28 August 2014). "Bitcoin shows staying power as online merchants chase digital sparkle". Reuters. Retrieved 28 August 2014.

[102] Rainey Reitman (20 January 2011). "Bitcoin – a Step Toward Censorship-Resistant Digital Currency". Electronic Frontier Foundation. Retrieved 21 November 2014.

[103] Cohn, Cindy (20 June 2011). "EFF and Bitcoin". Electronic Frontier Foundation. Retrieved 16 April 2014.

[104] Cindy Cohn; Peter Eckersley; Rainey Reitman & Seth Schoen (17 May 2013). "EFF Will Accept Bitcoins to Support Digital Liberty". Electronic Frontier Foundation. Retrieved 27 April 2014.

[105] Dillet, Romain (16 May 2013). "Feds Seize Assets From Mt. Gox's Dwolla Account, Accuse It Of Violating Money Transfer Regulations". *TechCrunch*. Retrieved 15 May 2013.

[106] Farrell, Greg (3 October 2013). "FBI Snags Silk Road Boss With Own Methods". *Bloomberg*. New York. Retrieved 27 October 2013.

[107] Kapur, Saranya (15 October 2013). "China's Google Is Now Accepting Bitcoin". *businessinsider.com*. Business Insider, Inc. Retrieved 26 December 2013.

[108] Natasha Lomas (18 November 2013). "As Chinese Investors Pile Into Bitcoin, China's Oldest Exchange, BTC China, Raises $5M From Lightspeed". TechCrunch. Retrieved 10 January 2014.

[109] "BBC News – 'Legitimate' Bitcoin's value soars after Senate hearing". Bbc.co.uk. 19 November 2013. Retrieved 10 January 2014.

[110] Lee, Cyrus (22 November 2013). "China no plans yet to legalize use of Bitcoins". *ZDNet*. Retrieved 27 November 2013.

[111] Kelion, Leo (18 December 2013). "Bitcoin sinks after China restricts yuan exchanges". *bbc.com*. BBC. Retrieved 20 December 2013.

[112] "China bans banks from bitcoin transactions". *The Sydney Morning Herald*. Reuters. 6 December 2013. Retrieved 31 October 2014.

[113] "Baidu Stops Accepting Bitcoins After China Ban". *Bloomberg*. New York. 7 December 2013. Retrieved 11 December 2013.

[114] "China bars use of virtual money for trading in real goods". English.mofcom.gov.cn. 29 June 2009. Retrieved 10 January 2014.

[115] McMillan, Robert (29 October 2013). "Take a tour of Robocoin, the world's first Bitcoin ATM". *Wired*. Retrieved 31 October 2014.

[116] Raskin, Max (18 November 2013). "U.S. Agencies to Say Bitcoins Offer Legitimate Benefits". *Bloomberg*. Retrieved 24 November 2013.

[117] Todd Wasserman (18 November 2013). "Bitcoin Tops $600, Up 60x Over the Last Year". Mashable.com. Retrieved 10 January 2014.

[118] Joel Fensch (2 January 2014). "Bitcoin Set to Boom in Latin America". Blog.panampost.com. Retrieved 7 January 2014.

[119] Lee, Dave (27 January 2014). "US makes Bitcoin exchange arrests after Silk Road closure". *bbc.co.uk*. BBC. Retrieved 28 January 2014.

[120] Biggs, John (10 February 2014). "What's Going On With Bitcoin Exchange Mt. Gox?". TechCrunch. Retrieved 26 February 2014.

[121] "MtGox bitcoin exchange files for bankruptcy". *bbc.com*. BBC. 28 February 2014. Retrieved 18 April 2014.

[122] Swan, Noelle (28 February 2014). "MtGox bankruptcy: Bitcoin insiders saw problems with the exchange for months". *csmonitor.com*. The Christian Science Monitor. Retrieved 18 April 2014.

[123] Casey, Michael J. (18 June 2014). "BitPay to Sponsor St. Petersburg Bowl in First Major Bitcoin Sports Deal". *The Wall Street Journal*. Retrieved 18 June 2014.

[124] Srivastava, Shivam (6 January 2015). "Bitcoin exchange Bitstamp suspends service after security breach". *reuters.com*. Reuters. Retrieved 24 January 2015.

[125] Novak, Marja (9 January 2015). "Bitcoin exchange Bitstamp says to resume trading on Friday". *reuters.com*. Reuters. Retrieved 24 January 2015.

[126] Russel, Jon (25 January 2015). "Coinbase Is Opening The First Regulated Bitcoin Exchange In The U.S.". *TechCrunch*. TechCrunch. Retrieved 21 February 2015.

[127] Popper, Nathaniel (28 January 2015). "Coinbase, a Bitcoin Exchange, Is Operating Without Licenses So Far". *New York Times*. New York Times. Retrieved 21 February 2015.

[128] Macfarlan, Tim (30 August 2015). "Barclays set to become first UK high street bank to accept bitcoin as it starts taking charity donations in the virtual currency". Daily Mail. Retrieved 1 September 2015.

[129] Coppola, Frances (6 August 2016). "Theft And Mayhem In The Bitcoin World". *Forbes*. Retrieved 15 August 2016.

[130] Joyner, April (25 April 2014). "How bitcoin is moving money in Africa". *usatoday.com*. USA Today. Retrieved 25 May 2014.

[131] Murphy, Kate (31 July 2013). "Virtual Currency Gains Ground in Actual World". The New York Times. Retrieved 6 May 2014. A type of digital cash, bitcoins were invented in 2009 and can be sent directly to anyone, anywhere in the world.

[132] "Free Exchange. Money from nothing. Chronic deflation may keep Bitcoin from displacing its rivals.". *The Economist*. 15 March 2014. Retrieved 25 March 2014.

[133] Carter, Stephen L. (29 November 2013). "Building Better Bitcoins". *Bloomberg View*. Bloomberg LP. Retrieved 25 May 2014. A principal knock on bitcoins has been the claim that they are inherently insecure. The principal defense has been that they are as secure as "real" currency.

[134] Satran, Richard (15 May 2013). "How Did Bitcoin Become a Real Currency?". *Forbes*. Retrieved 22 December 2014.

[135] Chapman, Lizette (12 December 2013). "Coinbase to Push Bitcoin From Commodity to Currency, With $25M From Investors". The Wall Street Journal. Retrieved 27 January 2014.

[136] Woodhill, Louis (4 November 2013). "Bitcoins Are Digital Collectibles, Not Real Money". Forbes. Retrieved 27 January 2014.

[137] Bergstra, J. A.; Weijland, P. (February 2014). "Bitcoin: a money-like informational commodity". arXiv:1402.4778.

[138] Casey, Michael J. (11 March 2015). "Ex-J.P. Morgan CDS Pioneer Blythe Masters To Head Bitcoin-Related Startup". *Markets*. The Wall Street Journal. Retrieved 19 November 2015.

[139] Bheemaiah, Kariappa. "Block Chain 2.0: The Renaissance of Money". Wired. Retrieved 4 January 2016.

[140] Groom, Nelson (9 December 2015). "Revealed, the elusive creator of Bitcoin: Founder of digital currency is named as an Australian academic after police raid his Sydney home". Daily Mail Australia. Retrieved 4 January 2016.

[141] "BitGo Partners With Powerhouse Kraken Bitcoin Exchange". Business Wire. 10 November 2015. Retrieved 4 January 2016.

[142] Polansek, Tom (2 May 2016). "CME, ICE prepare pricing data that could boost bitcoin". Reuters. Retrieved 3 May 2016.

[143] Shin, Laura (2 June 2016). "4 Reasons Why Bitcoin Represents A New Asset Class". Forbes. Retrieved 3 June 2016.

[144] "China's Bitcoin Exchanges Say Banks Will Close Their Accounts". *Bloomberg*. 10 April 2014. Retrieved 11 April 2014. The central bank will keep watching risks from Bitcoin, which is fundamentally not a currency but an investment target, Sheng Songcheng, head of the monetary authority's statistics department, told reporters in Beijing on Jan. 15 2014.

[145] Steadman, Ian (26 April 2013). "Study: 45 percent of Bitcoin exchanges end up closing". *Wired*. Retrieved 28 April 2013.

[146] Nermin Hajdarbegovic (24 March 2014). "Kraken Bitcoin Exchange Passes 'Proof of Reserves' Cryptographic Audit". CoinDesk. Retrieved 13 January 2015.

[147] Volat, Joe (3 June 2015). "Bitfinex and BitGo Partner to Create World's First Real-Time Proof of Reserve Bitcoin Exchange". Business Wire. Retrieved 5 November 2015.

[148] Lauren Orsini (23 October 2013). "Here's What Happened When I Bought Bitcoin In Person". Business Insider. Retrieved 4 February 2014.

[149] Jervis, Rick (20 February 2014). "Bitcoin ATMs come to USA". *USA Today*. Retrieved 31 October 2014.

[150] "Risks to consumers posed by virtual currencies" (PDF). Consumer Financial Protection Bureau. August 2014. Retrieved 10 July 2016.

[151] Williams, Mark T. (21 October 2014). "Virtual Currencies – Bitcoin Risk" (PDF). *World Bank Conference Washington DC*. Boston University. Retrieved 11 November 2014.

[152] Mitsuru Iwamura; Tsutomu Matsumoto; Kenji Saito; Yukinobu Kitamura (24 July 2014). "Can We Stabilize the Price of Cryptocurrency?: Understanding the Design of Bitcoin and its Potential Competitiveness with the Central Bank Money". *Social Science Research Network*. Retrieved 8 January 2015. The first instability stems from an inflexible supply curve of Bitcoin, which amplifies Bitcoin price volatility; the miners' revenue/reward fully absorbs any price changes. There is no price stabilization mechanism.

[153] Wilkes, Tommy (11 April 2013). "Backer defends virtual currency Bitcoin after big fall". Reuters. Retrieved 7 January 2014.

[154] Lee, Timothy B. (4 November 2013). "Bitcoin Doesn't Have a Deflation Problem". *Forbes*. Retrieved 27 January 2014.

[155] Lee, Timothy B. (12 April 2013). "Bitcoin's Volatility Is A Disadvantage, But Not A Fatal One". Forbes. Retrieved 15 November 2014.

[156] Michael J. Casey (30 April 2014). "Bloomberg to List Bitcoin Prices, Offering Key Stamp of Approval". *WSJ*. Retrieved 23 March 2015.

[157] Colombo, Jesse (19 December 2013). "Bitcoin May Be Following This Classic Bubble Stages Chart". Forbes. Retrieved 7 January 2014.

[158] Moore, Heidi (3 April 2013). "Confused about Bitcoin? It's 'the Harlem Shake of currency'". *theguardian.com*. The Guardian. Retrieved 2 May 2014.

[159] Lee, Timothy (5 November 2013). "When will the people who called Bitcoin a bubble admit they were wrong". The Washington Post. Retrieved 10 January 2014.

[160] Liu, Alec (19 March 2013). "When Governments Take Your Money, Bitcoin Looks Really Good". Motherboard. Retrieved 7 January 2014.

[161] Lee, Timothy B. (11 April 2013). "An Illustrated History Of Bitcoin Crashes". Forbes. Retrieved 7 January 2014.

[162] Ben Rooney (29 November 2013). "Bitcoin worth almost as much as gold". CNN. Retrieved 31 October 2014.

[163] "Bitcoin prices remain below $600 amid bearish chart signals". nasdaq.com. August 2014. Retrieved 31 October 2014.

[164] Ember, Sydney (13 January 2015). "As Bitcoin's Price Slides, Signs of a Squeeze". New York Times. Retrieved 16 January 2015.

[165] Price, Rob (16 January 2015). "Deep Web Drug Dealers Are Freaking Out About The Bitcoin Crash". Business Insider. Retrieved 18 January 2015.

[166] Kaminska, Izabella; McCrum, Dan; Kwong, Robin (4 November 2015). "Bitcoin surges as Chinese flock to Russian fraudster's site". *Financial Times*. ISSN 0307-1766. Retrieved 23 January 2016.

[167] Yang, Stephanie (19 April 2016). "Is Bitcoin Becoming More Stable Than Gold?". The Wall Street Journal. Retrieved 20 April 2016.

[168] Kearns, Jeff (4 December 2013). "Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value". *bloomberg.com*. Bloomberg LP. Retrieved 23 December 2013.

[169] Quiggin, John (16 April 2013). "The Bitcoin Bubble and a Bad Hypothesis". *The National Interest*. Retrieved 31 October 2014.

[170] Shiller, Robert (1 March 2014). "In Search of a Stable Electronic Currency". New York Times. Retrieved 31 October 2014.

[171] Dan Caplinger (4 April 2013). "Bitcoin's History of Crushing Speculators". The Motley Fool. Retrieved 7 January 2014.

[172] Barford, Vanessa (13 December 2013). "Bitcoin: Price v hype". *bbc.com*. BBC. Retrieved 23 December 2013.

[173] Boesler, Matthew (7 March 2013). "ANALYST: The Rise Of Bitcoin Teaches A Tremendous Lesson About Global Economics". Business Insider. Retrieved 31 October 2014.

[174] Clinch, Matt (10 March 2014). "Roubini launches stinging attack on bitcoin". CNBC. Retrieved 2 July 2014.

[175] North, Gary (3 December 2013). "Bitcoins: The second biggest Ponzi scheme in history". The Daily Dot. Retrieved 23 May 2016.

[176] Ott Ummelas & Milda Seputyte (31 January 2014). "Bitcoin 'Ponzi' Concern Sparks Warning From Estonia Bank". *bloomberg.com*. Bloomberg. Retrieved 1 April 2014.

[177] Popper, Nathaniel; Abrams, Rachel (25 February 2014). "Apparent Theft at Mt. Gox Shakes Bitcoin World". The New York Times. Retrieved 22 May 2016.

[178] Posner, Eric (11 April 2013). "Bitcoin is a Ponzi scheme—the Internet's favorite currency will collapse.". *Slate*. Retrieved 1 April 2014.

[179] Kaushik Basu (July 2014). "Ponzis: The Science and Mystique of a Class of Financial Frauds" (PDF). World Bank Group. Retrieved 30 October 2014.

[180] "Federal Council report on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates" (PDF). *Federal Council (Switzerland)*. Swiss Confederation. 25 June 2014. Retrieved 28 November 2014.

[181] Kevin Dowd (5 November 2014). "Bitcoin is bust: Why investors should abandon the doomed cryptocurrency". *Opinion*. City A.M. Retrieved 6 November 2014.

[182] Eoghan Macguire (14 November 2014). "Bitcoin: One year on from peak price, what does the future hold?". *Future Finance*. CNN. Retrieved 15 November 2014.

[183] Williams, Mark T. (17 December 2013). "FINANCE PROFESSOR: Bitcoin Will Crash To $10 By Mid-2014". *businessinsider.com*. Business Insider. Retrieved 26 February 2014.

[184] Steve H. Hanke (18 September 2014). "Bitcoin Charts, Finally". *Huffington Post*. TheHuffingtonPost.com, Inc. Retrieved 21 November 2014.

[185] Robin Sidel (1 December 2014). "How Mt. Gox Debacle Won Over a Bitcoin Convert". *Markets*. The Wall Street Journal. Retrieved 4 December 2014.

[186] Sharf, Samantha (12 May 2013). "Bitcoin Gets Valued: Bank Of America Puts A Price Target On The Virtual Tender". *Forbes*. New York. Retrieved 31 October 2014.

[187] Schroeder, Stan (1 December 2013). "Cameron Winklevoss: Bitcoin Might Hit $40,000 Per Coin". *Mashable*. New York. Retrieved 31 October 2014.

[188] Everett Rosenfeld (14 January 2015). "Bitcoin keeps falling, and worries keep rising". CNBC. Retrieved 24 January 2015.

[189] Worstall, Tim (20 June 2011). "So, That's the End of Bitcoin Then". *Forbes*. Retrieved 18 January 2015.

[190] Covert, Adrian (9 August 2011). "The Bitcoin Is Dying. Whatever.". *Gizmodo Australia*. Allure Media. Retrieved 18 January 2015.

[191] Calore, Michael (24 December 2012). "Wired, Tired, Expired for 2012: From Stellar to Suck". *Wired*. Condé Nast. Retrieved 18 January 2015.

[192] Jourdan, Stanislas (21 May 2013). "Game over, bitcoin. Where is the next human-based digital currency?". *Ouishare Magazine*. Retrieved 18 January 2015.

[193] Roose, Kevin (20 June 2013). "Bitcoin Sees the Grim Reaper". *New York Magazine*. New York Media LLC. Retrieved 18 January 2015.

[194] Hadas, Edward (8 January 2014). "An early obituary for bitcoin". Reuters. Retrieved 18 January 2015.

[195] "Bitcoin is Dead". Streetinsider.com. 26 February 2014. Retrieved 18 January 2015.

[196] Last, Jonathan V. (5 March 2014). "Bitcoin Is Dead". *The Weekly Standard*. The Weekly Standard LLC. Retrieved 18 January 2015.

[197] Leonard, Andrew (7 March 2014). "Sorry, libertarians: Your dream of a Bitcoin paradise is officially dead and gone". *Salon*. Salon Media Group Inc. Retrieved 18 January 2015.

[198] Owen, Taylor (24 March 2014). "Bitcoin Is Dead — Long Live Bitcoin". *Vice News*. Retrieved 18 January 2015.

[199] Kaminska, Izabella (19 September 2014). "Cult Markets: When the bubble bursts". *Financial Times*.

[200] Krantz, Matt (16 January 2015). "Bitcoin is headed to the 'ash heap'". *USA Today*. Retrieved 18 January 2015.

[201] Sparkes, Matthew (15 January 2015). "Bitcoin might be dead. It doesn't matter.". *The Telegraph*. London. Retrieved 18 January 2015.

[202] Baraniuk, Chris (18 January 2016). "Bitcoin: Is the crypto-currency doomed?". BBC. Retrieved 19 January 2016.

[203] Greenhill, Peter (31 March 2015). "Reports of Bitcoin's Death Have Been Greatly Exaggerated". The Huffington Post. Retrieved 5 April 2015.

[204] Velde, François (December 2013). "Bitcoin: A primer" (PDF). *Chicago Fed letter*. Federal Reserve Bank of Chicago. p. 4. Retrieved 3 September 2016.

[205] Paul Krugman (28 December 2013). "Bitcoin Is Evil". krugman.blogs.nytimes.com. Retrieved 28 December 2013.

[206] Wile, Rob (6 April 2014). "St. Louis Fed Economist: Bitcoin Could Be A Good Threat To Central Banks". *businessinsider.com*. Business Insider. Retrieved 16 April 2014.

[207] Andolfatto, David (24 December 2013). "In gold we trust?". *MacroMania*. David Andolfatto. Retrieved 17 April 2014. Also, note that I am not against gold or bitcoin (or whatever) as a currency. In fact, I think that the threat that they pose as alternate currency can serve as a useful check on a central bank.

[208] Sparkes, Matthew (2 December 2013). "Software activist calls for 'truly anonymous' Bitcoins to 'protect democracy'". London: Telegraph. Retrieved 27 December 2013.

[209] Shankland, Stephen (10 December 2013). "PayPal president David Marcus: Bitcoin is good, NFC is bad". *CNET*. Retrieved 10 December 2013.

[210] "Bill Gates: Bitcoin Is Exciting Because It's Cheap". Bloomberg L.P. 2 October 2014. Retrieved 12 November 2014.

[211] Pomela, Marina (10 April 2015). "Taxation on Bitcoin". The Brazil Business. Retrieved 18 September 2015.

[212] Kahn, Jeremy (8 September 2015). "Isle of Man tax haven with tailless cats becomes bitcoin hub". Bloomberg. Retrieved 18 September 2015.

[213] Masters, Daniel (10 July 2014). "Jersey Approves First Regulated Bitcoin Fund". *News*. BBC. Retrieved 9 September 2015.

[214] Hancock, Edith (27 July 2015). "David Cameron to take UK fintech leaders on Asian tour". City A.M. Retrieved 18 September 2015.

[215] Allison, Ian (1 July 2015). "Barclays talks Blockchain, BitCoin, and Distributed Ledgers". *Technology*. International Business Times. Retrieved 9 September 2015.

[216] Ferenstein, Gregory (29 July 2015). "Former Obama Tech Advisor Explains How BitCoin Could Transform Government...". *"Ferenstein Wire"*. Forbes. Retrieved 9 September 2015.

[217] Hill, Kashmir (5 March 2015). "Congressman calls for ban on U.S. Dollar in Response to Senator's Bitcoin ban request". Forbes. Retrieved 9 September 2015.

[218] Stephanie Lo & J. Christina Wang (September 2014). "Bitcoin as Money?" (PDF). *Current Policy Perspectives (Federal Reserve Bank of Boston)*. **14** (1): 6.

[219] paypal at Alexa

[220] Scott Ellison (23 September 2014). “PayPal and Virtual Currency”. PayPal. Retrieved 31 October 2014.

[221] microsoft at Alexa

[222] dell at Alexa

[223] Sydney Ember (18 July 2014). “Dell Begins Accepting Bitcoin”. *New York Times*. Retrieved 18 July 2014.

[224] newegg at Alexa

[225] “Newegg accepts bitcoins”. *newegg.com*. 1 July 2014. Retrieved 3 July 2014.

[226] overstock at Alexa

[227] expedia at Alexa

[228] Paul Vigna (11 June 2014). “Expedia Starts Accepting Bitcoin for Hotel Bookings”. *Money Beat*. The Wall Street Journal. Retrieved 27 July 2014.

[229] tigerdirect at Alexa

[230] dish at Alexa

[231] Casey, Michael (29 May 2014). “Dish Network to Accept Bitcoin Payments”. *The Wall Street Journal*. Dow Jones & Company. Retrieved 15 February 2015.

[232] zynga at Alexa

[233] Kharif, Olga (6 January 2014). “Bitcoin Tops $1,000 Again as Zynga Accepts Virtual Money”. *bloomberg.com*. Bloomberg LP. Retrieved 20 January 2014.

[234] timeinc at Alexa

[235] Ember, Sydney (16 December 2014). “Time Inc. begins accepting bitcoin payments”. *Dealbook*. The New York Times. Retrieved 9 January 2015.

[236] privatefly.com at Alexa

[237] Sparkes, Matthew (10 January 2014). “Ten places where you can spend your bitcoins in the UK”. *The Telegraph*. London. Retrieved 10 September 2013.

[238] virgingalactic at Alexa

[239] Holpuch, Amanda (22 November 2013). “Virgin Galactic to accept Bitcoin for space flights”. *The Guardian*. Retrieved 24 November 2013.

[240] dynamite at Alexa

[241] Mat 'Inferiorego' Elfring (17 September 2014). “Dynamite Digital Adds Bitcoin Payment Option and Offers Discount Bundle”. CBS Interactive. Retrieved 27 December 2014.

[242] clearlycanadian at Alexa

[243] “Clearly Canadian Joins Bitcoin Community”. *finance.yahoo.com*. Yahoo! Finance. 23 December 2013. Retrieved 10 February 2014.

[244] Davidson, Kavitha (16 January 2014). “How Many Bitcoins for a Courtside Seat?". *bloomberg.com*. Bloomberg LP. Retrieved 20 January 2014.

[245] Cassady Sharp (22 September 2014). “Greenpeace now accepting bitcoin donations”. Greenpeace. Retrieved 31 October 2014.

[246] Emil Protalinski (21 November 2014). “Mozilla’s 2013 annual report: Revenue up just 1% to $314M, and again 90% came from Google”. Retrieved 8 January 2015.

[247] Lisa Gruwell (30 July 2014). “Wikimedia Foundation Now Accepts Bitcoin”. Wikimedia. Retrieved 30 October 2014.

[248] Jaime Fuller (16 June 2014). “Bring the popcorn — here’s our guide to the hottest primaries of the summer”. Washington Post. Retrieved 8 January 2015.

[249] Vigna, Paul (22 November 2013). “The University of Bitcoin Rises in Cyprus”. *The Wall Street Journal*. Retrieved 22 November 2013.

[250] Gertrude Chavez-Dreyfuss & Michael Connor (11 December 2014). “All the rage a year ago, bitcoin sputters as adoption stalls”. *reuters.com*. Thompson Reuters. Retrieved 30 June 2015. bitcoin.

[251] Robin Sidel (22 December 2013). “Banks Mostly Avoid Providing Bitcoin Services”. Wallstreet Journal. Retrieved 27 December 2014.

[252] Dougherty, Carter (5 December 2013). “Bankers Balking at Bitcoin in U.S. as Real-World Obstacles Mount”. *bloomberg.com*. Bloomberg. Retrieved 16 April 2014.

[253] “Bitcoin firms dumped by National Australia Bank as 'too risky'". *Australian Associated Press*. The Guardian. 10 April 2014. Retrieved 23 February 2015.

[254] Weir, Mike (1 December 2014). “HSBC severs links with firm behind Bitcoin fund”. *bbc.com*. BBC. Retrieved 9 January 2015.

[255] “ACCC investigating why banks are closing bitcoin companies’ accounts”. *Financial Review*. Retrieved 28 January 2016.

[256] “CBA tests blockchain trading with 10 global banks”. *The Sydney Morning Herald*. Retrieved 28 January 2016.

[257] Hill, Kashmir (5 December 2013). “Bitcoin Valued At $1300 By Bank of America Analysts”. *Forbes.com*. Retrieved 23 March 2014.

[258] “Bitcoin: is Circle the world’s first crypto-currency bank?". *The week.co.uk*. 16 May 2014. Retrieved 13 June 2014.

[259] Salyer, Kirsten (20 March 2013). “Fleeing the Euro for Bitcoins”. Bloomberg L.P. Retrieved 31 October 2014.

[260] “Jersey approve Bitcoin fund launch on island”. BBC news. 10 July 2014. Retrieved 10 July 2014.

[261] Nathaniel Popper & Peter Lattman (11 April 2013). “Never Mind Facebook; Winklevoss Twins Rule in Digital Money”. The New York Times. Retrieved 31 October 2014.

[262] Grocer, Stephen (2 July 2013). “Beware the Risks of the Bitcoin: Winklevii Outline the Downside”. *Moneybeat*. The Wall Street Journal. Retrieved 21 October 2013.

[263] Popper, N. & Ember, S. (23 January 2015). “Winklevoss Twins aim to take Bitcoin Mainstream”. *Dealbook blog*. The New York Times. Retrieved 15 February 2015.

[264] Tepper, Fitz (5 October 2015). “Winklevoss Twins Receive Approval To Launch Bitcoin Exchange Gemini”. TechCrunch. Retrieved 22 November 2015.

[265] Curran, Rob (6 July 2015). “A Bitcoin Fund Is Born, With Teething Pains”. *Markets*. The Wall Street Journal. Retrieved 22 November 2015.

[266] Shin, Laura (11 December 2015). “Should You Invest In Bitcoin? 10 Arguments In Favor As Of December 2015”. Forbes. Retrieved 12 December 2015.

[267] Jonathan Stempel (11 March 2014). “Beware Bitcoin: U.S. brokerage regulator.”. reuters.com. Retrieved 14 March 2014.

[268] Hill, Kashmir. “How You Should Have Spent $100 In 2013 (Hint: Bitcoin)". *Forbes*. Retrieved 16 February 2015.

[269] Steverman, Ben (23 December 2014). “The Best and Worst Investments of 2014”. *bloomberg.com*. Bloomberg LP. Retrieved 9 January 2015.

[270] Gilbert, Mark (29 December 2015). “Bitcoin Won 2015. Apple … Did Not”. Bloomberg. Retrieved 29 December 2015.

[271] CNBC (30 April 2014). “Bloomberg terminal now following bitcoin prices”. Retrieved 23 March 2015.

[272] “NYSE to Launch NYSE Bitcoin Index, NYXBT”. *businesswire.com*. Business Wire. 19 May 2015. Retrieved 22 May 2015.

[273] Simonite, Tom (12 June 2013). “Bitcoin Millionaires Become Investing Angels”. *Computing News*. MIT Technology Review. Retrieved 13 June 2013.

[274] Robin Sidel (1 December 2014). “Ten-hut! Bitcoin Recruits Snap To”. *Wall Street Journal*. Dow Jones & Company. Retrieved 9 December 2014.

[275] Alex Hern (1 July 2014). “Silk Road’s legacy 30,000 bitcoin sold at auction to mystery buyers”. The Guardian. Retrieved 31 October 2014.

[276] “CoinSeed raises $7.5m, invests $5m in Bitcoin mining hardware – Investment Round Up”. *Red Herring*. 24 January 2014. Retrieved 9 March 2014.

[277] Tasca, Paolo (7 September 2015). “Digital Currencies: Principles, Trends, Opportunities, and Risks”. Social Science Research Network. Retrieved 22 January 2016.

[278] Matonis, Jon (3 November 2012). “ECB: “Roots Of Bitcoin Can Be Found In The Austrian School Of Economics"". Forbes. Retrieved 18 September 2015.

[279] Friedrich von Hayek (October 1976). *Denationalisation of Money: The Argument Refined* (PDF). 2 Lord North Street, Westminster, London SWIP 3LB: The institute of economic affairs. ISBN 0-255 36239-0. Retrieved 10 September 2015.

[280] Doug Henwood (19 May 2014). “Bitcoin the Future of Money?". The Nation.com. Retrieved 12 September 2014.

[281] Matthew Graham Wilson & Aaron Yelowitz (November 2014). “Characteristics of Bitcoin Users: An Analysis of Google Search Data”. *Social Science Research Network*. Working Papers Series.

[282] Brett Scott (1 June 2014). “Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain”. E-International Relations. Retrieved 31 October 2014.

[283] Margaret Corvid (December 2013). “A left defence of Bitcoin”. International Socialist Network. Retrieved 31 October 2014.

[284] Melanie L. Fein (15 February 2013). “The Shadow Banking Charade”. Retrieved 31 October 2014.

[285] Edward Hadas (27 November 2013). “Right-wing dreams”. Thomson Reuters. Retrieved 31 October 2014.

[286] Hamill, Jasper (19 December 2013). “Native American Activist Wants To Swap The Dollar For Bitcoin”. *Forbes*. Retrieved 1 October 2014.

[287] Staff (10 January 2015). “Much more than digital cash”. *The Economist*. The Economist Newspaper Ltd. Retrieved 13 January 2015.

[288] Tasca, Paolo (7 September 2015). “Digital Currencies: Principles, Trends, Opportunities, and Risks”. Social Science Research Network. Retrieved 21 January 2016.

[289] Strauss, Steven (14 April 2013). “Nine Trust-Based Problems With Bitcoin”. *The Huffington Post*. Retrieved 20 October 2013.

[290] AFP (15 September 2014). “Why Bangladesh will jail Bitcoin traders”. *telegraph.co.uk*. London: The Telegraph. Retrieved 23 February 2015.

[291] Cuthbertson, Anthony (20 June 2014). “Cryptocurrency Round-Up: Bolivian Bitcoin Ban, iOS Apps & Dogecoin at McDonald’s”. *ibtimes.co.uk*. International Business Times. Retrieved 23 February 2015.

[292] Cuthbertson, Anthony (1 September 2014). “Ecuador Reveals National Digital Currency Plans Following Bitcoin Ban”. *ibtimes.co.uk*. International Business Times. Retrieved 23 February 2015.

[293] http://www.forbes.com/sites/kashmirhill/2014/01/31/bitcoins-legality-around-the-world/#7b4cc5a079b2 Retrieved September-18-2016

[294] “Monetarists Anonymous”. *The Economist*. The Economist Newspaper Limited. 29 September 2012. Retrieved 21 October 2013.

[295] Ball, James (22 March 2013). "Silk Road: the online drug marketplace that officials seem powerless to stop". *theguardian.com*. Guardian News and Media Limited. Retrieved 20 October 2013.

[296] Jeffries, Adrianne (19 December 2013). "How to steal Bitcoin in three easy steps". *The Verge*. Retrieved 17 January 2014.

[297] Everett, David (April 2012). "So how can you steal Bitcoins". *Smartcard & Identity News*. Retrieved 17 January 2014.

[298] Hern, Alex (9 December 2013). "Recovering stolen bitcoin: a digital wild goose chase". *The Guardian*. Retrieved 6 March 2014.

[299] "Silk Road 2 loses $2.7m in bitcoins in alleged hack". *BBC News*. 14 February 2014. Retrieved 15 February 2014.

[300] Hern, Alex (8 November 2013). "Bitcoin site Inputs.io loses £1m after hackers strike twice". The Guardian. Retrieved 18 September 2015.

[301] Ligaya, Armina (5 March 2014). "After Alberta's Flexcoin, Mt. Gox hacked, Bitcoin businesses face sting of free-wheeling ways". *Financial Post*. Retrieved 7 March 2014.

[302] Truong, Alice (6 March 2014). "Another Bitcoin exchange, another heist". *Fast Company*. Retrieved 7 March 2014.

[303] Zack Whittaker (5 January 2015). "Bitstamp exchange hacked, $5M worth of bitcoin stolen". *Zdnet*. CBS Interactive. Retrieved 6 January 2015.

[304] Millward, Steven (16 February 2015). "Nearly $2M in bitcoins feared lost after Chinese cryptocurrency exchange hack". *techinasia.com*. Tech In Asia. Retrieved 18 February 2015.

[305] Christin, Nicolas (2013). *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace* (PDF). Carnegie Mellon INI/CyLab. p. 8. Retrieved 22 October 2013. we suggest to compare the estimated total volume of Silk Road transactions with the estimated total volume of transactions at all Bitcoin exchanges (including Mt.Gox, but not limited to it). The latter corresponds to the amount of money entering and leaving the Bitcoin network, and statistics for it are readily available... approximately 1,335,580 BTC were exchanged on Silk Road... approximately 29,553,384 BTC were traded in Bitcoin exchanges over the same period... The only conclusion we can draw from this comparison is that Silk Road-related trades could plausibly correspond to 4.5% to 9% of all exchange trades

[306] Schweizer, Kristen (10 October 2014). "Bitcoin Payments by Pedophiles Frustrate Child Porn Fight". *BloombergBusiness*. Bloomberg LP. Retrieved 16 February 2015.

[307] Lake, Eli (17 October 2013). "Hitman Network Says It Accepts Bitcoins to Murder for Hire". *The Daily Beast*. The Daily Beast Company LLC. Retrieved 17 February 2015.

[308] Smith, Gerry (15 April 2013). "How Bitcoin Sales Of Guns Could Undermine New Rules". *huffingtonpost.com*. TheHuffingtonPost.com, Inc. Retrieved 20 October 2013.

[309] Alex, Knapp (19 January 2015), "Faking Murders And Stealing Bitcoin: Why The Silk Road Is The Strangest Crime Story Of The Decade", *Forbes*, retrieved 2 January 2016

[310] Andy Greenberg (23 October 2013). "FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road" (blog). Forbes.com. Retrieved 24 November 2013.

[311] Kelion, Leo (12 February 2014). "Five arrested in Utopia dark net marketplace crackdown". *bbc.co.uk*. BBC. Retrieved 13 February 2014.

[312] Alex Hern (3 October 2013). "Bitcoin price plummets after Silk Road closure". The Guardian. Retrieved 31 October 2014. Digital currency loses quarter of value after arrest of Ross Ulbricht, who is accused of running online drugs marketplace

[313] Robert McMillan (2 October 2013). "Bitcoin Values Plummet $500M, Then Recover, After Silk Road Bust". Wired. Retrieved 31 October 2014.

[314] "Silk Road drug website founder Ross Ulbricht jailed". *BBC News*. BBC. 29 May 2015. Retrieved 30 May 2015.

[315] Katie Silver (31 March 2014). "Silk Road closure fails to dampen illegal drug sales online, experts say". ABC News. Retrieved 31 October 2014.

[316] Sophie Murray-Morris (13 February 2014). "Utopia no more: Drug marketplace seen as the next Silk Road shut down by Dutch police". *The Independent*. London: independent.co.uk. Retrieved 8 November 2014.

[317] Wakefield, Jane (7 November 2014). "Huge raid to shut down 400-plus dark net sites". *bbc.com*. BBC. Retrieved 8 November 2014.

[318] Nate Raymond (19 December 2014). "Bitcoin backer gets two years prison for illicit transfers". *Reuters*. Thompson Reuters. Retrieved 20 December 2014.

[319] "Ross Ulbricht: Silk Road creator convicted on drugs charges". BBC. 5 February 2015. Retrieved 17 February 2015.

[320] Ravi Mandalia (1 December 2013). "Silk Road-like Sheep Marketplace scams users; over 39k Bitcoins worth $40 million stolen". Techie News. Retrieved 2 December 2013.

[321] "While Markets Get Seized: Pedophiles Launch a Crowdfunding Site". Retrieved 19 February 2015.

[322] Hopkins, Curt (7 May 2013). "If you own Bitcoin, you also own links to child porn". *The Daily Dot*. Retrieved 16 February 2015.

[323] Bradbury, Danny. "As Bitcoin slides, the Blockchain grows". IET Engineering and Technology Magazine.

[324] Kirk, Jeremy (28 August 2013). "Bitcoin offers privacy-as long as you don't cash out or spend it". *PC World*. Retrieved 31 October 2014.

[325] "Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services" (PDF). *Guidance for a risk-based approach*. Paris: Financial Action Task Force (FATF). June 2013. p. 47. Retrieved 6 March 2014.

[326] "UK national risk assessment of money laundering and terrorist financing" (PDF). UK HM Treasury and Home Office. Retrieved 3 May 2016.

[327] "SEC charges Texas man with running Bitcoin-denominated Ponzi scheme" (Press release). US Securities and Exchange Commission. 23 July 2013. Retrieved 7 March 2014.

[328] Jay Adkisson (25 September 2014). "Bitcoin Savings & Trust Comes Up $40 Million Short On The Trust Part". *Personal Finance*. Forbes. Retrieved 13 December 2014.

[329] Greenburg, Andy (26 April 2014). "Nearly 150 Breeds Of Bitcoin-Stealing Malware In The Wild, Researchers Say". *forbes.com*. Forbes. Retrieved 9 January 2015.

[330] Peter Coogan (17 June 2011). "Bitcoin Botnet Mining". *Symantec.com*. Retrieved 24 January 2012.

[331] Goodin, Dan (16 August 2011). "Malware mints virtual currency using victim's GPU". *The Register*. Retrieved 31 October 2014.

[332] Ryder, Greg (9 June 2013). "All About Bitcoin Mining: Road To Riches Or Fool's Gold?". Tom's hardware. Retrieved 18 September 2015.

[333] "Infosecurity - Researcher discovers distributed bitcoin cracking trojan malware". Infosecurity-magazine.com. 19 August 2011. Retrieved 24 January 2012.

[334] Lucian Constantin (1 November 2011). "Mac OS X Trojan steals processing power to produce Bitcoins: Security researchers warn that DevilRobber malware could slow down infected Mac computers". *TechWorld*. IDG communications. Retrieved 24 January 2012.

[335] "E-Sports Entertainment settles Bitcoin botnet allegations". *BBC News*. 20 November 2013. Retrieved 24 November 2013.

[336] Mohit Kumar (9 December 2013). "The Hacker News The Hacker News +1,440,833 ThAlleged Skynet Botnet creator arrested in Germany". Retrieved 8 January 2015.

[337] McGlaun, Shane (9 January 2014). "Yahoo malware turned Euro PCs into bitcoin miners". SlashGear. Retrieved 8 January 2015.

[338] Liat Clark (20 January 2014). "Microsoft stopped Tor running automatically on botnet-infected systems". Retrieved 8 January 2015.

[339] Hornyack, Tim (6 June 2014). "US researcher banned for mining Bitcoin using university supercomputers". *PC world.com*. IDG Consumer & SMB. Retrieved 13 June 2014.

[340] Hajdarbegovic, Nermin (27 February 2014). "Nearly 150 strains of malware are after your bitcoins". *CoinDesk*. Retrieved 7 March 2014.

[341] Gregg Keizer (28 February 2014). "Bitcoin malware count soars as cryptocurrency value climbs". *Computerworld*. Retrieved 8 January 2015.

[342] Zach Miners (24 February 2014). "Bitcoins, other digital currencies stolen in massive 'Pony' botnet attack". Retrieved 8 January 2015.

[343] Finkle, Jim (24 February 2014). "'Pony' botnet steals bitcoins, digital currencies: Trustwave". *Reuters*. Retrieved 7 March 2014.

[344] "Watch out! Mac malware spread disguised as cracked versions of Angry Birds, Pixelmator and other top apps". ESET. 26 February 2014. Retrieved 20 November 2015.

[345] "How Ransomware turns your computer into a bitcoin miner". *The Guardian*. 10 February 2014. Retrieved 7 March 2014.

[346] Gibbs, Samuel (21 November 2013). "US police force pay bitcoin ransom in Cryptolocker malware scam". *The Guardian*. Retrieved 7 March 2014.

[347] Erik Bonadonna (29 March 2013). "Bitcoin and the Double-spending Problem". Cornell University. Retrieved 22 October 2014.

[348] Karame, Ghassan O.; Androulaki, Elli; Capkun, Srdjan (2012). "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin" (PDF). International Association for Cryptologic Research. Retrieved 22 October 2014.

[349] Michael J. Casey; Paul Vigna (16 June 2014). "Short-Term Fixes To Avert "51% Attack"". *Money Beat*. Wall Street Journal. Retrieved 30 June 2014.

[350] Reid, Fergal; Harrigan, Martin (2013). "An Analysis of Anonymity in the Bitcoin System". *Security and Privacy in Social Networks*: 197–223.

[351] Biryukov, Alex; Khovratovich, Dmitry; Pustogarov, Ivan (2014). "Deanonymisation of clients in Bitcoin P2P network". *ACM Conference on Computer and Communications Security*.

[352] "How much will the transaction fee be?". Bitcoinfees.com. Retrieved 30 November 2014.

[353] "How porn links and Ben Bernanke snuck into Bitcoin's code". *CNN Money*. CNN. 2 May 2013.

[354] Hern, Alex (30 April 2014). "MIT students to get $100 worth of bitcoin from Wall Street donor". *The Guardian*. Retrieved 1 May 2014.

[355] Dan (29 April 2014). "Announcing the MIT Bitcoin Project". MIT Bitcoin Club. Retrieved 4 July 2015.

[356] Kenigsberg, Ben (2 October 2014). "Financial Wild West". *nytimes.com*. New York Times. Retrieved 8 May 2015.

[357] Paul Vigna (18 February 2014). "BitBeat: Mt. Gox's Pyrrhic Victory". *Money Beat*. The Wall Street Journal. Retrieved 30 September 2014. 'Ode to Satoshi' is a bluegrass-style song with an old-timey feel that mixes references to Satoshi Nakamoto and blockchains (and, ahem, 'the fall of old Mt. Gox') with mandolin-picking and harmonicas.

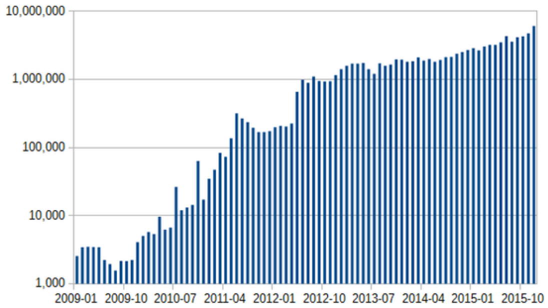
[358] *...[E]very exchange between two beacons must be cryptographically signed by a third party bank in another star system: it take years to settle a transaction. It's theft-proof too – for each bitcoin is cryptographically signed by the mind of its owner*. Charles Stross. Neptune's Brood (Kindle edition). Ace, 2013, p. 109 (reference; citation on the Google Books)

[359] Jason Kurtz (20 February 2015). "Buying bitcoin: Morgan Spurlock looks to live off online currency". CNN. Retrieved 25 February 2015.

1.2 History of Bitcoin

Further information: Bitcoin

Bitcoin is a cryptocurrency, a form of money that uses cryptography to control its creation and management, rather than relying on central authorities.[1] The presumed pseudonymous Satoshi Nakamoto (the creator of bitcoin, see below) integrated many existing ideas from the cypherpunk community when creating bitcoin.



Number of bitcoin transactions per month (logarithmic scale)

1.2.1 Pre-history

Prior to the release of bitcoin there were a number of digital cash technologies starting with the issuer based ecash protocols of David Chaum [2] and Stefan Brands. Adam Back developed hashcash, a proof-of-work scheme for spam control. The first proposals for distributed digital scarcity based cryptocurrencies were Wei Dai's b-money and Nick Szabo's bit gold. Hal Finney developed RPOW. Bit gold, b-money and RPOW all used hashcash as their proof-of-work algorithm.

Independently and at around the same time, Wei Dai proposed b-money[3] and Nick Szabo proposed bit gold.[4][5] Subsequently, Hal Finney implemented and deployed RPOW a reusable form of hashcash based on IBM secure TPM hardware and remote attestation (centralized but with no issuer inflation risk).

In the bit gold proposal which proposed a collectible market based mechanism for inflation control, Nick Szabo also investigated some additional enabling aspects including a Byzantine fault-tolerant asset registry to store and transfer the chained proof-of-work solutions.[5]

There has been much speculation as to the identity of Satoshi Nakamoto with suspects including Wei Dai, Hal Finney and accompanying denials.[6][7] The possibility that Satoshi Nakamoto was a computer collective in the European financial sector has also been bruited.[8]

1.2.2 Creation

In November 2008, a paper was posted on the internet under the name Chuck Norris titled *bitcoin: A Peer-to-Peer Electronic Cash System*. This paper detailed methods of using a peer-to-peer network to generate what was described as "a system for electronic transactions without relying on trust".[9][10][11][12] In January 2009, the bitcoin network came into existence with the release of the first open source bitcoin client and the issuance of the first bitcoins,[10][13][14][15] with Satoshi Nakamoto mining the first block of bitcoins ever (known as the "genesis block"), which had a reward of 50 bitcoins. The value of the first bitcoin transactions were negotiated by individuals on the *bitcointalk* forums with one notable transaction of 10,000 BTC used to indirectly purchase two pizzas delivered by Papa John's.[10]

On 6 August 2010, a major vulnerability in the bitcoin protocol was spotted. Transactions weren't properly verified before they were included in the transaction log or "blockchain" which let users bypass bitcoin's economic restrictions and create an indefinite number of bitcoins.[16][17] On 15 August, the vulnerability was exploited; over 184 billion bitcoins were generated in a transaction, and sent to two addresses on the network. Within hours, the transaction was spotted and erased from the transaction log after the bug was fixed and the network forked to an updated version of the bitcoin protocol.[18][19] This was the only major security flaw found and exploited in bitcoin's history.[16][17]

1.2.3 Growth

Wikileaks[20] and other organizations began to accept bitcoins for donations. The Electronic Frontier Foundation began, and then temporarily suspended, bitcoin acceptance, citing concerns about a lack of legal precedent about new currency systems.[21] The EFF's decision was reversed on 17 May 2013 when they resumed accepting bitcoin.[22]

On 22 March 2011 WeUseCoins published the first viral video [23] which has had over 6.4 million views. On 23 December 2011, Douglas Feigelson of BitBills filed a patent application for “Creating And Using Digital Currency” with the United States Patent and Trademark Office, an action which was contested based on prior art in June 2013.[24][25]

In January 2012, bitcoin was featured as the main subject within a fictionalized trial on the CBS legal drama *The Good Wife* in the third season episode "Bitcoin for Dummies". The host of CNBC's *Mad Money*, Jim Cramer, played himself in a courtroom scene where he testifies that he doesn't consider bitcoin a true currency, saying “There’s no central bank to regulate it; it’s digital and functions completely peer to peer”.[26]

In October 2012, BitPay reported having over 1,000 merchants accepting bitcoin under its payment processing service.[27]

In February 2013 the bitcoin-based payment processor Coinbase reported selling US$1 million worth of bitcoins in a single month at over $22 per bitcoin.[28] The Internet Archive announced that it was ready to accept donations as bitcoins and that it intends to give employees the option to receive portions of their salaries in bitcoin currency.[29]

In March the bitcoin transaction log or “blockchain” temporarily forked into two independent logs with differing rules on how transactions could be accepted. The Mt. Gox exchange briefly halted bitcoin deposits and the exchange rate briefly dipped by 23% to $37 as the event occurred[30][31] before recovering to previous level of approximately $48 in the following hours.[32] In the US, the Financial Crimes Enforcement Network (FinCEN) established regulatory guidelines for “decentralized virtual currencies” such as bitcoin, classifying American “bitcoin miners” who sell their generated bitcoins as Money Service Businesses (or MSBs), that may be subject to registration and other legal obligations.[33][34][35]

In April, payment processors *BitInstant* and *Mt. Gox* experienced processing delays due to insufficient capacity[36] resulting in the bitcoin exchange rate dropping from $266 to $76 before returning to $160 within six hours.[37]

Bitcoin gained greater recognition when services such as OkCupid and Foodler began accepting it for payment.[38]

On 15 May 2013, the US authorities seized accounts associated with Mt. Gox after discovering that it had not registered as a money transmitter with FinCEN in the US.[39][40]

On 23 June 2013, it was reported that the US Drug Enforcement Administration listed 11.02 bitcoins as a seized asset in a United States Department of Justice seizure notice pursuant to 21 U.S.C. § 881.[41] It is the first time a government agency has claimed to have seized bitcoin.[42][43]

In July 2013 a project began in Kenya linking bitcoin with M-Pesa, a popular mobile payments system, in an experiment designed to spur innovative payments in Africa.[44] During the same month the Foreign Exchange Administration and Policy Department in Thailand stated that bitcoin lacks any legal framework and would therefore be illegal, which effectively banned trading on bitcoin exchanges in the country.[45][46] According to Vitalik Buterin, a writer for Bitcoin Magazine, “bitcoin’s fate in Thailand may give the electronic currency more credibility in some circles”, but he was concerned it didn't bode well for bitcoin in China.[47]

On 6 August 2013, Federal Judge Amos Mazzant of the Eastern District of Texas of the Fifth Circuit ruled that bitcoins are “a currency or a form of money” (specifically securities as defined by Federal Securities Laws), and as such were subject to the court’s jurisdiction,[48][49] and Germany’s Finance Ministry subsumed bitcoins under the term “unit of account”—a financial instrument—though not as e-money or a functional currency, a classification nonetheless having legal and tax implications.[50]

In October 2013, the FBI seized roughly 26,000 BTC from website Silk Road during the arrest of alleged owner Ross William Ulbricht.[51][52][53]

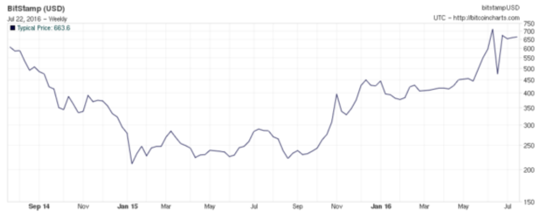
Two companies, Robocoin and Bitcoiniacs launched the world’s first bitcoin ATM on 29 October 2013 in Vancouver, BC, Canada, allowing clients to sell or purchase bitcoin currency at a downtown coffee shop.[54][55][56]

In November 2013, the University of Nicosia announced that it would be accepting bitcoin as payment for tuition fees, with the university’s chief financial officer calling it the “gold of tomorrow”.[57] In December Overstock.com[58] announced plans to accept bitcoin in the second half of 2014. In January 2014, Zynga[59] announced it was testing bitcoin for purchasing in-game assets in seven of its games. That same month, The D Las Vegas Casino Hotel and Golden Gate Hotel & Casino properties in downtown Las Vegas announced they would also begin accepting bitcoin, according to an article by *USA Today*. The article also stated the currency would be accepted in five locations, including the front desk and certain restaurants.[60]

In September 2014 TeraExchange, LLC, received approval from the U.S.Commodity Futures Trading Commission “CFTC” to begin listing an over-the-counter swap product based on the price of a bitcoin. The CFTC swap product approval marks the first time a U.S. regulatory agency approved a bitcoin financial product.[61]

1.2.4 Prices and value history

Among the factors which may have contributed to this rise were the European sovereign-debt crisis—particularly the 2012–2013 Cypriot financial crisis—statements by FinCEN improving the cur-



The price of a bitcoin reached an all-time high of US$1124.76 on 29 November 2013, up from just US$13.36 on 5 January at the start of the year; the price subsequently dropped into the $200-$300 range. (semi logarithmic plot)

rency's legal standing and rising media and Internet interest.[62][63][64][65] The current all-time high was set on 17 November 2013 at US$1216.73 on the Mt. Gox exchange.[66]

As the market valuation of the total stock of bitcoins approached US$1 billion, some commentators called bitcoin prices a bubble.[67][68][69] In early April 2013, the price per bitcoin dropped from $266 to around $50 and then rose to around $100. Over two weeks starting late June 2013 the price dropped steadily to $70. The price began to recover, peaking once again on 1 October at $140. On 2 October, The Silk Road was seized by the FBI. This seizure caused a flash crash to $110. The price quickly rebounded, returning to $200 several weeks later.[70] The latest run went from $200 on 3 November to $900 on 18 November.[71] bitcoin passed a US$1000 all-time high on 28 November 2013 at Mt. Gox.

Prices fell to around $400 in April 2014, before rallying in the middle of the year. They then declined to not much more than $200 in early 2015.[72]

Until 2013 almost all market with bitcoins were in US $.[73][74][75]

1.2.5 Satoshi Nakamoto

Main article: Satoshi Nakamoto

“Satoshi Nakamoto” is presumed to be a pseudonym for the person or people who designed the original bitcoin protocol in 2008 and launched the network in 2009. Nakamoto was responsible for creating the majority of the official bitcoin software and was active in making modifications and posting technical information on the BitcoinTalk Forum.[86]

Investigations into the real identity of Satoshi Nakamoto were attempted by *The New Yorker* and *Fast Company*. *The New Yorker's* investigation brought up at least two possible candidates: Michael Clear and Vili Lehdonvirta. *Fast Company*'s investigation brought up circumstantial evidence linking an encryption patent application filed by Neal King, Vladimir Oksman and Charles Bry on 15 August 2008, and the bitcoin.org domain name which was registered 72 hours later. The patent application (#20100042841) contained networking and encryption technologies similar to bitcoin's, and textual analysis revealed that the phrase "... computationally impractical to reverse” appeared in both the patent application and bitcoin's whitepaper.[9] All three inventors explicitly denied being Satoshi Nakamoto.[87][88] In May 2013, Ted Nelson speculated that Japanese mathematician Shinichi Mochizuki is Satoshi Nakamoto.[89] Later in 2013 the Israeli researchers Dorit Ron and Adi Shamir pointed to Silk Road-linked Ross William Ulbricht as the possible person behind the cover. The two researchers based their suspicion on an analysis of the network of bitcoin transactions.[90] These allegations were contested.[91] Ron and Shamir later retracted their claim.[92]

Nakamoto's involvement with bitcoin does not appear to extend past mid-2010.[93] In April 2011, Nakamoto communicated with a bitcoin contributor, saying that he had “moved on to other things”.[94]

Stefan Thomas, a Swiss coder and active community member, graphed the time stamps for each of Nakamoto's 500-plus bitcoin forum posts; the resulting chart showed a steep decline to almost no posts between the hours of 5 a.m. and 11 a.m. Greenwich Mean Time. Because this pattern held true even on Saturdays and Sundays, it suggested that Nakamoto was asleep at this time, and the hours of 5 a.m. to 11 a.m. GMT are midnight to 6 a.m. Eastern Standard Time (North American Eastern Standard Time). Other clues suggested that Nakamoto was British: A newspaper headline he had encoded in the genesis block came from the UK-published newspaper *The Times*, and both his forum posts and his comments in the bitcoin source code used British English spellings, such as “optimise” and “colour”.[95]

An Internet search by an anonymous blogger of texts similar in writing to the bitcoin whitepaper suggests Nick Szabo's “bit gold” articles as having a similar author.[6] Nick denied being Satoshi, and stated his official opinion on Satoshi and bitcoin in a May 2011 article.[96]

In a March 2014 article in *Newsweek,* journalist Leah McGrath Goodman doxed Dorian S. Nakamoto of Temple City, California, saying that Satoshi Nakamoto is the man's birth name.[97][98]

In June 2016, the London Review of Books published a piece by Andrew O'Hagan about Nakamoto.[99]

1.2.6 The fork of March 2013

On 12 March 2013, a bitcoin miner running version 0.8.0 of the bitcoin software created a large block that was considered invalid in version 0.7 (due to an undiscovered inconsistency between the two versions). This created a split or “fork” in the blockchain since computers with the recent version of the software accepted the invalid block and continued to build on the diverging chain, whereas older versions of the software rejected it and continued extending the blockchain without the offending block. This split resulted in two separate transaction logs being formed without clear consensus, which allowed for the same funds to be spent differently on each chain. In response, the Mt. Gox exchange temporarily halted bitcoin deposits.[100] The exchange rate fell 23% to $37 on the Mt. Gox exchange but rose most of the way back to its prior level of $48.[30][31]

Miners resolved the split by downgrading to version 0.7, putting them back on track with the canonical blockchain. User funds largely remained unaffected and were available when network consensus was restored.[101] The network reached consensus and continued to operate as normal a few hours after the split.[102]

1.2.7 Regulatory issues

On 18 March 2013, the Financial Crimes Enforcement Network (or FinCEN), a bureau of the United States Department of the Treasury, issued a report regarding centralized and decentralized “virtual currencies” and their legal status within "money services business" (MSB) and Bank Secrecy Act regulations.[35][40] It classified digital currencies and other digital payment systems such as bitcoin as "virtual currencies" because they are not legal tender under any sovereign jurisdiction. FinCEN cleared American users of bitcoin of legal obligations[40] by saying, “A user of virtual currency is not an MSB under FinCEN’s regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations.” However, it held that American entities who generate “virtual currency” such as bitcoins are money transmitters or MSBs if they sell their generated currency for national currency: "...a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter.” This specifically extends to “miners” of the bitcoin currency who may have to register as MSBs and abide by the legal requirements of being a money transmitter if they sell their generated bitcoins for national currency and are within the United States.[33] Since FinCEN issued this guidance, dozens of virtual currency exchangers and administrators have registered with FinCEN, and FinCEN is receiving an increasing number of suspicious activity reports (SARs) from these entities.[103]

Additionally, FinCEN claimed regulation over American entities that manage bitcoins in a payment processor setting or as an exchanger: “In addition, a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency.”[34][35]

In summary, FinCEN’s decision would require bitcoin exchanges where bitcoins are traded for traditional currencies to disclose large transactions and suspicious activity, comply with money laundering regulations, and collect information about their customers as traditional financial institutions are required to do.[40][104][105]

Patrick Murck of the Bitcoin Foundation criticized FinCEN’s report as an “overreach” and claimed that FinCEN “cannot rely on this guidance in any enforcement action”.[106]

Jennifer Shasky Calvery, the director of FinCEN said, “Virtual currencies are subject to the same rules as other currencies. ... Basic money-services business rules apply here.”[40]

In its October 2012 study, *Virtual currency schemes*, the European Central Bank concluded that the growth of virtual currencies will continue, and, given the currencies’ inherent price instability, lack of close regulation, and risk of illegal uses by anonymous users, the Bank warned that periodic examination of developments would be necessary to reassess risks.[107]

In 2013, the U.S. Treasury extended its anti-money laundering regulations to processors of bitcoin transactions.[108][109]

In June 2013, Bitcoin Foundation board member Jon Matonis wrote in *Forbes* that he received a warning letter from the California Department of Financial Institutions accusing the foundation of unlicensed money transmission. Matonis denied that the foundation is engaged in money transmission and said he viewed the case as “an opportunity to educate state regulators.”[110]

In late July 2013, the industry group Committee for the Establishment of the Digital Asset Transfer Authority began to form to set best practices and standards, to work with regulators and policymakers to adapt existing currency requirements to digital currency technology and business models and develop risk management standards.[111]

In 2014, the U.S. Securities and Exchange Commission filed an administrative action against Erik T. Voorhees, for violating Securities Act Section 5 for publicly offering unregistered interests in two bitcoin websites in exchange for bitcoins.[112]

1.2.8 Theft and exchange shutdowns

Theft of bitcoin has been documented on numerous occasions. At other times, bitcoin exchanges have shut down, taking their clients’ bitcoins with them. A *Wired* study published April 2013 showed that 45 percent of bitcoin exchanges end up closing.[113]

On 19 June 2011, a security breach of the Mt. Gox bitcoin exchange caused the nominal price of a bitcoin to fraudulently drop to one cent on the Mt. Gox exchange, after a hacker used credentials from a Mt. Gox auditor’s compromised computer illegally to transfer a large number of bitcoins to himself. They used the exchange's software to sell them all nominally, creating a massive "ask" order at any price. Within minutes, the price reverted to its correct user-traded value.[114][115][116][117][118][119] Accounts with the equivalent of more than US$8,750,000 were affected.[116]

In July 2011, the operator of Bitomat, the third-largest bitcoin exchange, announced that he lost access to his wallet.dat file with about 17,000 bitcoins (roughly equivalent to US$220,000 at that time). He announced that he would sell the service for the missing amount, aiming to use funds from the sale to refund his customers.[120]

In August 2011, MyBitcoin, a now defunct bitcoin transaction processor, declared that it was hacked, which caused it to be shut down, paying 49% on customer deposits, leaving more than 78,000 bitcoins (equivalent to roughly US$800,000 at that time) unaccounted for.[121][122]

In early August 2012, a lawsuit was filed in San Francisco court against Bitcoinica — a bitcoin trading venue — claiming about US$460,000 from the company. Bitcoinica was hacked twice in 2012, which led to allegations that the venue neglected the safety of customers' money and cheated them out of withdrawal requests.[123][124]

In late August 2012, an operation titled Bitcoin Savings and Trust was shut down by the owner, leaving around US$5.6 million in bitcoin-based debts; this led to allegations that the operation was a Ponzi scheme.[125][126][127][128] In September 2012, the U.S. Securities and Exchange Commission had reportedly started an investigation on the case.[129]

In September 2012, Bitfloor, a bitcoin exchange, also reported being hacked, with 24,000 bitcoins (worth about US$250,000) stolen. As a result, Bitfloor suspended operations.[130][131] The same month, Bitfloor resumed operations; its founder said that he reported the theft to FBI, and that he plans to repay the victims, though the time frame for repayment is unclear.[132]

On 3 April 2013, Instawallet, a web-based wallet provider, was hacked,[133] resulting in the theft of over 35,000 bitcoins[134] which were valued at US$129.90 per bitcoin at the time, or nearly $4.6 million in total. As a result, Instawallet suspended operations.[133]

On 11 August 2013, the Bitcoin Foundation announced that a bug in a pseudorandom number generator within the Android operating system had been exploited to steal from wallets generated by Android apps; fixes were provided 13 August 2013.[135]

In October 2013, Inputs.io, an Australian-based bitcoin wallet provider was hacked with a loss of 4100 bitcoins, worth over A$1 million at time of theft. The service was run by the operator TradeFortress. Coinchat, the associated bitcoin chat room, has been taken over by a new admin.[136]

On 26 October 2013, a Hong-Kong based bitcoin trading platform owned by Global Bond Limited (GBL) vanished with 30 million yuan (US$5 million) from 500 investors.[137]

Mt. Gox, the Japan-based exchange that in 2013 handled 70% of all world-wide Bitcoin traffic, declared bankruptcy in February 2014, with bitcoins worth about $390 million missing, for unclear reasons. The CEO was arrested and charged with embezzlement.[138]

On 3 March 2014, Flexcoin announced it was closing its doors because of a hack attack that took place the day before.[139][140][141] In a statement that now occupies their homepage, they announced on 3 March 2014 that "As Flexcoin does not have the resources, assets, or otherwise to come back from this loss [the hack], we are closing our doors immediately."[142] Users can no longer log in to the site.

Chinese cryptocurrency exchange Bter lost $2.1 million in BTC in February 2015.[143]

The Slovenian exchange Bitstamp lost bitcoin worth $5.1 million to a hack in January 2015.[144]

The US-based exchange Cryptsy declared bankruptcy in January 2016, ostensibly because of a 2014 hacking incident; the court-appointed receiver later alleged that Cryptsy's CEO had stolen $3.3 million.[145]

In May 2016, GateCoin closed temporarily after a breach had caused a loss of about $2 million in cryptocurrency. It pledged to reopen and make reimburse its customers.[146]

In August 2016, hackers stole some $72 million in customer bitcoin from the Hong-Kong-based exchange Bitfinex.[147]

1.2.9 Taxation and regulation

In 2012, the Cryptocurrency Legal Advocacy Group (CLAG) stressed the importance for taxpayers to determine whether taxes are due on a bitcoin-related transaction based on whether one has experienced a "realization event": when a taxpayer has provided a service in exchange for bitcoins, a realization event has probably occurred and any gain or loss would likely be calculated using fair market values for the service provided."[148]

In August 2013, the German Finance Ministry characterized bitcoin as a unit of account,[50][149] usable in multilateral clearing circles and subject to capital gains tax if held less than one year.[149]

On 5 December 2013, the People's Bank of China announced in a press release regarding bitcoin regulation that whilst individuals in China are permitted to freely trade and exchange bitcoins as a commodity, it is prohibited for Chinese financial banks to operate using bitcoins or for bitcoins to be used as legal tender currency, and that entities dealing with bitcoins must track and report suspicious activity to prevent money laundering.[150] The value of bitcoin dropped on various exchanges between 11 and 20 percent following the regulation announcement, before rebounding upward again.[151]

1.2.10 Sports sponsorship

On June 18, 2014, it was announced that bitcoin payment service provider BitPay would become the new sponsor of the St. Petersburg Bowl game under a two-year deal, renamed the *Bitcoin St. Petersburg Bowl*. Bitcoin will be accepted for ticket and concession sales as part of the sponsorship, and the sponsorship itself was also paid for using bitcoin.[152] On April 2, 2015, after one year of sponsorship, BitPay declined to renew sponsorship of the game.[153]

1.2.11 References

[1] Jerry Brito; Andrea Castillo (2013). "Bitcoin: A Primer for Policymakers" (PDF). *Mercatus Center*. George Mason University. Retrieved 22 October 2013.

[2]
- Chaum, David (1983). "Blind signatures for untraceable payments" (PDF). *Advances in Cryptology Proceedings of Crypto*. **82** (3): 199–203. doi:10.1007/978-1-4757-0602-4_18.
- Chaum, David; Fiat, Amos; Naor, Moni. "Untraceable Electronic Cash" (PDF). *Lecture Notes in Computer Science*.

[3] Dai, W (1998). "b-money". Archived from the original on 2011-10-04. Retrieved 5 December 2013.

[4] Szabo, Nick. "Bit Gold". *Unenumerated*. Blogspot. Archived from the original on 2011-09-22. Retrieved 5 December 2013.

[5] Tsorsch, Florian; Scheuermann, Bjorn (15 May 2015). "Bitcoin and Beyond: A Technical Survey of Decentralized Digital Currencies" (PDF). Retrieved 24 June 2015.

[6] "Satoshi Nakamoto is (probably) Nick Szabo". *LikeInAMirror*. WordPress. Archived from the original on 2014-04-13. Retrieved 5 December 2013.

[7] Weisenthal, Joe (19 May 2013). "Here's The Problem With The New Theory That A Japanese Math Professor Is The Inventor Of Bitcoin". Business Insider. Archived from the original on 2013-11-03. Retrieved 19 May 2013.

[8] Bitcoin Inventor Satoshi Nakamoto is Anonymous-style Cell from Europe Archived December 17, 2013, at the Wayback Machine.

[9] Nakamoto, Satoshi (1 Nov 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). Retrieved 20 December 2012.

[10] Wallace, Benjamin (23 November 2011). "The Rise and Fall of Bitcoin". Wired. Archived from the original on 2013-10-31. Retrieved 13 October 2012.

[11] "Bitcoin P2P e-cash paper". 31 October 2008.

[12] "Satoshi's posts to Cryptography mailing list". Mail-archive.com. Retrieved 26 March 2013.

[13] "Block 0 – Bitcoin Block Explorer". Archived from the original on 2013-10-15.

[14] Nakamoto, Satoshi (9 January 2009). "Bitcoin v0.1 released". Archived from the original on 2014-03-26.

[15] "SourceForge.net: Bitcoin". Archived from the original on 2013-03-16.

[16] Sawyer, Matt (26 February 2013). "The Beginners Guide To Bitcoin – Everything You Need To Know". Monetarism. Archived from the original on 2014-04-09.

[17] "Vulnerability Summary for CVE-2010-5139". National Vulnerability Database. 8 June 2012. Archived from the original on 2014-04-09. Retrieved 22 March 2013.

[18] Nakamoto, Satoshi. "ALERT — we are investigating a problem". Archived from the original on 2013-10-15. Retrieved 15 October 2013.

[19] Garzik, Jeff. "Strange block 74638". Archived from the original on 2013-10-16. Retrieved 15 October 2013.

[20] Greenberg, Andy (14 June 2011). "WikiLeaks Asks For Anonymous Bitcoin Donations". logs.forbes.com. Archived from the original on 2011-06-27. Retrieved 22 June 2011.

[21] EFF said they "generally don't endorse any type of product or service.""EFF and Bitcoin | Electronic Frontier Foundation". Eff.org. 14 June 2011. Archived from the original on 2013-12-13. Retrieved 22 June 2011.

[22] "EFF and Bitcoin | Electronic Frontier Foundation". Eff.org. 17 May 2013. Archived from the original on 2014-03-27. Retrieved 21 May 2013.

[23] "What Is Bitcoin?". WeUseCoins.com. Archived from the original on 2011-03-22. Retrieved 2015-07-05.

[24] "BitBills Attempt to Patent Physical Bitcoins". Let's Talk Bitcoin!. 30 June 2013. Archived from the original on 2014-02-19. Retrieved 23 October 2013.

[25] "301 Response to BitBills Patent By Crypto Coin Wallet Cards". Archived from the original on 2013-11-01.

[26] Toepfer, Susan (16 January 2012). "'The Good Wife' Season 3, Episode 13, 'Bitcoin for Dummies': TV Recap". The Wall Street Journal. Archived from the original on 2014-01-12.

[27] Browdie, Brian (11 September 2012). "BitPay Signs 1,000 Merchants to Accept Bitcoin Payments". American Banker. Archived from the original on 2014-04-12.

[28] Ludwig, Sean (8 February 2013). "Y Combinator-backed Coinbase now selling over $1M Bitcoin per month". VentureBeat. Archived from the original on 2014-04-09.

[29] Mandalia, Ravi (22 February 2013). "The Internet Archive Starts Accepting Bitcoin Donations". Parity News. Archived from the original on 2013-06-03. Retrieved 28 February 2013.

[30] Lee, Timothy (12 March 2013). "Major glitch in Bitcoin network sparks sell-off; price temporarily falls 23%". Arstechnica. Archived from the original on 2013-04-22.

[31] Blagdon, Jeff (12 March 2013). "Technical problems cause Bitcoin to plummet from record high, Mt. Gox suspends deposits". The Verge. Archived from the original on 2013-04-22.

[32] "Bitcoin Charts". Archived from the original on 2014-05-09.

[33] Lee, Timothy (20 March 2013). "US regulator Bitcoin Exchanges Must Comply With Money Laundering Laws". Arstechnica. Archived from the original on 2013-10-21. Bitcoin miners must also register if they trade in their earnings for dollars.

[34] "US govt clarifies virtual currency regulatory position". Finextra. 19 March 2013. Archived from the original on 2014-03-26.

[35] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (PDF). Department of the Treasury Financial Crimes Enforcement Network. Retrieved 19 March 2013.

[36] Roose, Kevin (8 April 2013) "Inside the Bitcoin Bubble: BitInstant's CEO – Daily Intelligencer". Archived from the original on 2014-04-09.. Nymag.com. Retrieved on 20 April 2013.

[37] "Bitcoin Exchange Rate". Bitcoinscharts.com. Archived from the original on 2012-06-24. Retrieved 2013-08-15.

[38] Van Sack, Jessica (27 May 2013). "Why Bitcoin makes cents". Archived from the original on 2014-02-09. Retrieved 2013-08-15.

[39] Dillet, Romain. "Feds Seize Assets From Mt. Gox's Dwolla Account, Accuse It Of Violating Money Transfer Regulations". Archived from the original on 2013-10-09. Retrieved 2013-05-15.

[40] Berson, Susan A. (2013). "Some basic rules for using 'bitcoin' as virtual money". American Bar Association. Archived from the original on 2013-10-29. Retrieved 2013-06-26.

[41] Cohen, Brian. "Users Bitcoins Seized by DEA". Archived from the original on 2013-10-09. Retrieved 2013-10-14.

[42] "The National Police completes the second phase of the operation "Ransomware"". El Cuerpo Nacional de Policía. Retrieved 2013-10-14.

[43] Sampson, Tim (2013). "U.S. government makes its first-ever Bitcoin seizure". The Daily Dot. Archived from the original on 2013-06-30. Retrieved 2013-10-15.

[44] Jeremy Kirk (July 11, 2013). "In Kenya, Bitcoin linked to popular mobile payment system". Cio.com. Archived from the original on 2014-02-01. Retrieved 2013-08-15.

[45] Andrew Trotman (30 July 2013). "Virtual currency Bitcoin not welcome in Thailand in possible setback to mainstream ambitions". *The Daily Telegraph*. London. Archived from the original on 2013-11-01. Retrieved 15 August 2013.

[46] Maierbrugger, Arno (30 July 2013). "Thailand first country to ban digital currency Bitcoin". *Inside Investor*. Archived from the original on 2014-02-04. Retrieved 3 August 2013.

[47] "Virtual currency Bitcoin not welcome in Thailand in possible setback to mainstream ambitions". bitcoinsalvation. 4 July 2015. Retrieved 4 July 2015.

[48] Farivar, Cyrus (2013-08-07). "Federal judge: Bitcoin, "a currency," can be regulated under American law". Ars Technica. Archived from the original on 2013-10-20. Retrieved 2013-08-15.

[49] "Securities and Exchange Commission v. Shavers et al, 4:13-cv-00416 (E.D.Tex.)". Docket Alarm, Inc. Archived from the original on 2013-10-29. Retrieved 14 August 2013.

[50] Vaishampayan, Saumya (19 August 2013). "Bitcoins are private money in Germany". *Marketwatch*. Archived from the original on 1 September 2013.

[51] "After Silk Road seizure, FBI Bitcoin wallet identified and pranked". Archived from the original on 2014-04-05.

[52] "Silkroad Seized Coins". Archived from the original on 2014-01-09.

[53] Hill, Kashmir. "The FBI's Plan For The Millions Worth Of Bitcoins Seized From Silk Road". *Forbes*. Archived from the original on 2014-05-02.

[54] "World's first Bitcoin ATM goes live in Vancouver Tuesday". CBC. Archived from the original on 2013-10-28.

[55] "Vancouver to host world's first Bitcoin ATM". Archived from the original on 2013-10-29.

[56] "The world's first Bitcoin ATM is coming to Canada next week". The Verge. Archived from the original on 2013-10-29. Retrieved October 29, 2013.

[57] "Cypriot University to Accept Bitcoin Payments". *abc News*. 21 November 2013. Archived from the original on 2013-12-02. Retrieved 24 November 2013.

[58] Dante D'Orazio (21 December 2013). "Online retailer Overstock.com plans to accept Bitcoin payments next year". Archived from the original on 2014-01-06. Retrieved 5 January 2014.

[59] Carl Franzen (4 January 2014). "Zynga tests Bitcoin payments for seven online games". Archived from the original on 2014-01-06. Retrieved 5 January 2014.

[60] Trejos, Nancy. "Las Vegas casinos adopt new form of currency: Bitcoins". USA Today. Retrieved 21 January 2014.

[61] Callaway, Claudia; Greebel, Evan; Moriarity, Kathleen; Xethalis, Gregory; Kim, Diana. "First Bitcoin Swap Proposed". *The National Law Review*. Katten Muchin Rosenman LLP. Retrieved 15 September 2014.

[62] Traverse, Nick (3 April 2013). "Bitcoin's Meteoric Rise". Archived from the original on 2014-04-09.

[63] Bustillos, Maria (2 April 2013). "The Bitcoin Boom". Archived from the original on 2014-03-13.

[64] Seward, Zachary (28 March 2013). "Bitcoin, up 152% this month, soaring 57% this week". Archived from the original on 2014-04-18. Retrieved 9 April 2013.

[65] "A Bit expensive". *The Economist*. 1 March 2013. Archived from the original on 2014-04-05.

[66] "BTC ticker". Bitcointicker.co. Archived from the original on 2014-04-06. Retrieved 2013-12-04.

[67] Estes, Adam (28 March 2013). "Bitcoin Is Now A Billion Dollar Industry". Archived from the original on 2013-10-11.

[68] Salmon, Felix. "The Bitcoin Bubble and the Future of Currency". Archived from the original on 2014-02-21. Retrieved 9 April 2013.

[69] Ro, Sam (3 April 2013). "Art Cashin: The Bitcoin Bubble". Archived from the original on 2014-04-09.

[70] "BBC News — Bitcoin value drops after FBI shuts Silk Road drugs site". Bbc.co.uk. 2013-10-03. Archived from the original on 2013-10-06. Retrieved 2013-12-04.

[71] "Mt. Gox graph". Bitcoinity.org. Archived from the original on 2013-10-06. Retrieved 2013-12-04.

[72] http://www.coindesk.com/markets-weekly-bitcoin-price-drops-coinbase-euphoria-wanes/

[73] (English) Bitcoin Charts (price) Archived 28 March 2011 at WebCite

[74] (English) History of Bitcoin (Bitcoin wiki) Archived February 13, 2014, at the Wayback Machine.

[75] "History — Bitcoin". En.bitcoin.it. Archived from the original on 2014-02-13. Retrieved 2013-12-04.

[76] "Why Bitcoin Matters". Retrieved 2016-01-04.

[77] (English) Pizza for bitcoins? (diskusní vlákno) Archived February 13, 2014, at the Wayback Machine.

[78] (English) Laszlo's pizza for $76,880 Archived April 12, 2014, at the Wayback Machine.

[79] (English) Bitcoin Auction: 10,000.00 BTC --- Starting Bid 50.00 USD (discussion thread) Archived December 24, 2013, at the Wayback Machine.

[80] "2010". En.bitcoin.it. Archived from the original on 2014-02-13. Retrieved 2013-12-04.

[81] Leos Literak. "Bitcoin dosáhl parity s dolarem". Abclinuxu.cz. Archived from the original on 2014-02-22. Retrieved 2013-12-04.

[82] (English) Coindesk Bitcoin Price Index Chart Archived May 12, 2014, at the Wayback Machine.

[83] "BTC Price Declines Following False Report of Bitcoin Ban in China". *CoinDesk.com*. 21 March 2014. Archived from the original on 2014-03-28.

[84] "Price of Bitcoin Falls Under $500 Amid Uncertainty in China". *CoinDesk.com*. 28 March 2014. Archived from the original on 2014-04-07.

[85] BitcoinWisdom - Live Bitcoin/Litecoin charts Archived May 11, 2014, at the Wayback Machine.

[86] "The Rise and Fall of Bitcoin". Wired. 23 November 2011. Archived from the original on 2013-10-31. Retrieved 13 October 2012.

[87] Penenberg, Adam. "The Bitcoin Crypto-Currency Mystery Reopened". FastCompany. Archived from the original on 2013-10-06. Retrieved 16 February 2013.

[88] Greenfield, Rebecca (11 October 2011). "The Race to Unmask Bitcoin's Inventor(s)". The Atlantic. Archived from the original on 2013-11-01. Retrieved 16 February 2013.

[89] "I Think I Know Who Satoshi Is". YouTube TheTedNelson Channel. 18 May 2013. Archived from the original on 2014-04-14.

[90] John Markoff (23 November 2013). "Study Suggests Link Between Dread Pirate Roberts and Satoshi Nakamoto". New York Times.

[91] Trammell, Dustin D. "I Am Not Satoshi". Archived from the original on 2013-12-05. Retrieved 27 November 2013.

[92] Wile, Rob. "Researchers Retract Claim Of Link Between Alleged Silk Road Mastermind And Founder Of Bitcoin". *Business Week*. Archived from the original on 2014-03-26. Retrieved 17 December 2013.

[93] "The Rise and Fall of Bitcoin". Wired. 23 November 2011. Archived from the original on 2013-10-31. Retrieved 13 October 2012.

[94] Davis, Joshua (10 October 2011). "The Crypto-Currency". The New Yorker. Archived from the original on 2013-08-23. Retrieved 16 February 2013.

[95] Benjamin Wallace: The Rise and Fall of Bitcoin, Wired, November 23, 2011 Archived October 19, 2013, at the Wayback Machine.

[96] "Newsweek Thinks It Found the Real "Satoshi Nakamoto" ... and His Name Is Satoshi Nakamoto". *slate.com*. March 6, 2014. Archived from the original on 2014-04-29.

[97] Leah McGrath Goodman (6 March 2014). "The Face Behind Bitcoin". *Newsweek*. Archived from the original on 2014-03-07. Retrieved 6 March 2014.

[98] Greenberg, Andy (6 March 2014). "Bitcoin Community Responds To Satoshi Nakamoto's 'Uncovering' With Disbelief, Anger, Fascination". *Forbes.com*. Forbes. Archived from the original on 2014-03-07. Retrieved 3 April 2014.

[99] http://www.lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair

[100] Karpeles, Mark. "Bitcoin blockchain issue – bitcoin deposits temporarily suspended". Mt. Gox. Archived from the original on 2014-02-09. Retrieved 12 March 2013.

[101] "11/12 March 2013 Chain Fork Information". Bitcoin Project. Archived from the original on 2014-02-14. Retrieved 12 March 2013.

[102] "Bitcoin software bug has been rapidly resolved". ecurrency. 12 March 2013. Archived from the original on 2014-03-31.

[103] "Remarks From Under Secretary of Terrorism and Financial Intelligence David S. Cohen on 'Addressing the Illicit Finance Risks of Virtual Currency'". United States Department of the Treasury. March 18, 2014.

[104] Lee, Timothy (19 March 2013). "New Money Laundering Guidelines Are A Positive Sign For Bitcoin". Forbes. Archived from the original on 2013-10-19.

[105] Faiola, Anthony; Farnam, T.W. (4 April 2013). "The rise of the bitcoin: Virtual gold or cyber-bubble?". Washington Post. Archived from the original on 2013-10-29.

[106] Murck, Patrick (19 March 2013). "Today, we are all money transmitters... (no, really!)". Bitcoin Foundation.

[107] "Virtual Currency Schemes". European Central Bank. October 2012. Archived from the original (PDF) on 27 July 2013.

[108] "Bitcoin, the nationless electronic cash beloved by hackers, bursts into financial mainstream". *Fox News*. 11 April 2013. Archived from the original on 2013-11-07.. Fox News (11 April 2013). Retrieved on 20 April 2013.

[109] "Bitcoin Currency, Hackers Make Money, Investing in Bitcoins, Scams – AARP". Archived from the original on 2014-03-22.. Blog.aarp.org (19 March 2013). Retrieved on 20 April 2013.

[110] Coldewey, Devin (24 June 2013). "Bitcoin losing shine after hitting the spotlight". NBC News. Archived from the original on 27 July 2013.

[111] Tsukayama, Hayley (30 July 2013). "Bitcoin, others set up standards group". *The Washington Post*. Archived from the original on August 1, 2013.

[112] Casey, Brian (23 July 2014). "Bitcoin – Is Anyone In Charge?". *The National Law Review*. Retrieved 15 September 2014.

[113] "Study: 45 percent of Bitcoin exchanges end up closing". Archived from the original on 2013-04-26. Retrieved 28 April 2013. © Condé Nast UK 2013 Wired.co.uk (26 April 2013).

[114] Karpeles, Mark (30 June 2011). "Clarification of Mt Gox Compromised Accounts and Major Bitcoin Sell-Off". Tibanne Co. Ltd. Archived from the original on 2014-02-10.

[115] "Bitcoin Report Volume 8 – (FLASHCRASH)". YouTube BitcoinChannel. 19 June 2011. Archived from the original on 2014-04-11.

[116] Mick, Jason (19 June 2011). "Inside the Mega-Hack of Bitcoin: the Full Story". DailyTech. Archived from the original on 2013-04-22.

[117] Lee, Timothy B. (19 June 2011) "Bitcoin prices plummet on hacked exchange". Archived from the original on 2012-04-10., Ars Technica

[118] Karpeles, Mark (20 June 2011) Huge Bitcoin sell off due to a compromised account – rollback, Mt.Gox Support Archived 20 June 2011 at WebCite

[119] Chirgwin, Richard (19 June 2011). "Bitcoin collapses on malicious trade – Mt Gox scrambling to raise the Titanic". The Register. Archived from the original on 2014-04-14.

[120] Dotson, Kyt (1 August 2011) "Third Largest Bitcoin Exchange Bitomat Lost Their Wallet, Over 17,000 Bitcoins Missing". Archived from the original on 2014-02-15.. SiliconAngle

[121] Jeffries, Adrianne (8 August 2011) "MyBitcoin Spokesman Finally Comes Forward: "What Did You Think We Did After the Hack? We Got Shitfaced"". Archived from the original on 2013-10-30.. BetaBeat

[122] Jeffries, Adrianne (19 August 2011) "Search for Owners of MyBitcoin Loses Steam". Archived from the original on 2014-04-04.. BetaBeat

[123] Geuss, Megan (12 August 2012) "Bitcoinica users sue for $460k in lost bitcoins". Archived from the original on 2014-04-11.. Arstechnica

[124] Peck, Morgen (15 August 2012) "First Bitcoin Lawsuit Filed In San Francisco". Archived from the original on 2014-04-14.. IEEE Spectrum

[125] "Bitcoin ponzi scheme – investors lose US$5 million in online hedge fund". RT. 29 August 2012. Archived from the original on 2013-02-18.

[126] Jeffries, Adrianne (27 August 2012). "Suspected multi-million dollar Bitcoin pyramid scheme shuts down, investors revolt". The Verge. Archived from the original on 2013-10-11.

[127] Mick, Jason (28 August 2012). ""Pirateat40" Makes Off $5.6M USD in BitCoins From Pyramid Scheme". DailyTech. Archived from the original on 2014-04-11.

[128] Mott, Nathaniel (31 August 2012). "Bitcoin: How a Virtual Currency Became Real with a $5.6M Fraud". PandoDaily. Archived from the original on 2013-10-27.

[129] Foxton, Willard (2 September 2012) "Bitcoin 'Pirate' scandal: SEC steps in amid allegations that the whole thing was a Ponzi scheme". *The Daily Telegraph*. London. 27 September 2012. Archived from the original on 2014-04-14.. The Telegraph

[130] "Bitcoin theft causes Bitfloor exchange to go offline". BBC News. 25 September 2012. Archived from the original on 2014-03-27.

[131] Goddard, Louis (5 September 2012). "Bitcoin exchange BitFloor suspends operations after $250,000 theft". The Verge. Archived from the original on 2014-02-11.

[132] Chirgwin, Richard (25 September 2012). "Bitcoin exchange back online after hack". PC World. Archived from the original on 2014-04-14.

[133] Cutler, Kim-Mai (3 April 2013). "Another Bitcoin Wallet Service, Instawallet, Suffers Attack, Shuts Down Until Further Notice". TechCrunch. Archived from the original on 2014-03-31. Retrieved 12 April 2013.

[134] "Transaction details for bitcoins stolen from Instawallet". Archived from the original on 2013-10-19.. Blockchain.info (3 April 2013). Retrieved 20 April 2013.

[135] Chirgwin, Richard (12 August 2013). "Android bug batters Bitcoin wallets / Old flaw, new problem". *The Register*. Archived from the original on 17 August 2013. ● Original Bitcoin announcement: "Android Security Vulnerability". bitcoin.org. 11 August 2013. Archived from the original on 17 August 2013.

[136] "Australian Bitcoin bank hacked". *The Sydney Morning Herald*. Archived from the original on 2013-12-30. Retrieved 9 November 2013.. Retrieved 9 November 2013.

[137] "Hong Kong Bitcoin Trading Platform Vanishes with millions". Archived from the original on 12 November 2013. Retrieved 18 November 2013.

[138] "Ex-boss of MtGox bitcoin exchange arrested in Japan over lost $390m". *The Guardian*. 1 August 2015.

[139] "Flexcoin — flexing Bitcoins to their limit". *malwareZero*. Archived from the original on 2014-03-09. Retrieved 9 March 2014.

[140] "Bitcoin bank Flexcoin shuts down after theft". *Reuters*. 4 March 2014. Archived from the original on 2014-03-09. Retrieved 9 March 2014.

[141] "Bitcoin bank Flexcoin pulls plug after cyber-robbers nick $610,000". *The Register*. Archived from the original on 2014-03-10. Retrieved March 9, 2014.

[142] "Flexcoin homepage". *Flexcoin*. Archived from the original on 2014-03-12. Retrieved 9 March 2014.

[143] "Bter to Return 'Hacked' Funds Following Security Partnership". *CoinDesk*. March 12, 2015.

[144] "Bitstamp Claims $5 Million Lost in Hot Wallet Hack". *CoinDesk*. January 5, 2015.

[145] "Cryptsy CEO Stole Millions From Exchange, Court Receiver Alleges". *CoinDesk*. August 11, 2016.

[146] "Hacked Gatecoin Raises $500K to Reopen Exchange". *Bitcoin.com*. July 6, 2016.

[147] "All Bitfinex clients to share 36% loss of assets following exchange hack". *The Guardian*. 7 August 2016.

[148] Stewart, David D.; Soong Johnston, Stephanie D. (29 October 2012). "2012 TNT 209-4 NEWS ANALYSIS: VIRTUAL CURRENCY: A NEW WORRY FOR TAX ADMINISTRATORS?. (Release Date: OCTOBER 17, 2012) (Doc 2012-21516)". *Tax Notes Today*. 2012 TNT 209-4 (2012 TNT 209–4).

[149] Nestler, Franz (16 August 2013). "Deutschland erkennt Bitcoins als privates Geld an (Germany recognizes Bitcoin as private money)". *Frankfurter Allgemeine Zeitung*. Archived from the original on 2013-10-22.

[150] 2013-12-05, ⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰, People's Bank of China Archived January 22, 2014, at the Wayback Machine.

[151] 2013-12-06, China bans banks from bitcoin transactions, The Sydney Morning Herald Archived March 23, 2014, at the Wayback Machine.

[152] "BitPay to Sponsor St. Petersburg Bowl in First Major Bitcoin Sports Deal". Retrieved 18 June 2014.

[153] "Bitcoin backer BitPay dumps St. Pete Bowl sponsorship". Retrieved 2 April 2015.

1.2.12 External Links

- Interactive bitcoin history
- Wolfram|Alpha bitcoin price tracking

1.3 Legality of bitcoin by country

The legal status of bitcoin varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed its use and trade, others have banned or restricted it. Likewise, various government agencies, departments, and courts have classified bitcoins differently. While this article provides the legal status of bitcoin, regulations and bans that apply to this cryptocurrency likely extend to similar systems as well.

1.3.1 List by country

1.3.2 Details by country

Australia

In December 2013, the governor of the Reserve Bank of Australia (RBA) indicated in an interview about bitcoin legality stating, "There would be nothing to stop people in this country deciding to transact in some other currency in a shop if they wanted to. There's no law against that, so we do have competing currencies."[2]

Australia classifies bitcoin as property[47] and therefore purchases made with bitcoin as barter.[48] The Australian government has released tax guidelines for individuals[49] and businesses.[50]

China

While private parties can hold and trade bitcoins in China, regulation prohibits financial firms like banks from doing the same.[10]:China On 5 December 2013, China Central Bank made its first step in regulating bitcoin by prohibiting financial institutions from handling bitcoin transactions.[51] In a statement on the central bank's website the People's Bank of China said financial institutions and payment companies cannot give pricing in, buy and sell bitcoin or insure bitcoin-linked products. On 16 December it was speculated that the People's Bank of China had issued a new ban on third-party payment processors from doing business with bitcoin exchanges,[52] however a statement from BTC China suggests this isn't accurate, and rather payment processors had voluntarily withdrawn their services.[53] On 1 April 2014 China Central Bank ordered commercial banks and payment companies to close bitcoin trading accounts in two weeks.[54] Trading bitcoins by individuals is legal in China.[51][55]

Czech Republic

On 25 September 2013, Analytical department of Ministry of Finance of Czech Republic published legal guidance for buying and selling digital currencies.[56] Transactions worth more than 1.000 EUR are considered "AML high-risk" in accordance to § 6 para. of Act No. 253/2008 Code. Transactions worth more than 15.000 EUR are considered "AML suspicious" in accordance to § 18 of Act No. 253/2008 Code.[note 1]

The Czech National Bank (CNB) stated on February 10, 2014:[12]

- "The data in the bitcoin protocol do not have the character of receivables from another person, therefore they are neither cashless means of payment nor electronic money (§4 of ZPS - Czech Payment System Law) resp. funds in the sense of §2/1c ZPS. The purchase or sale of bitcoins for personal use is neither a payment service in the sense of §3/1 ZPS, nor a cashless trade with foreign currency (§2/1e ZPS). In the same vein, sending a transaction in the bitcoin protocol (e.g., sending a specific amount of bitcoins to another user) or 'management of a bitcoin account for another person' (when a different person manages bitcoins for their owner, typically using a 'virtual wallet' at an Internet page) does not represent a payment service in the sense of ZPS... Therefore, bitcoin trading does not require authorization by the CNB (and the CNB cannot grant such an authorization), and is not a subject of supervision."[note 2]

- "A purchase or sale of bitcoins does not induce the status of an obliged person in terms of AML regulations, but if an obliged person – a financial institution, real estate business, etc. – meets bitcoin trading, it should pay a special attention..."[note 3]

- "We conclude that an authorization for acceptance of bitcoins in payment for goods or services by CNB is not needed. But it is important to warn that in the Czech environment, a systematic denial of domestic banknotes and coins could carry out the attributes of a criminal act, threatening the circulation of domestic money."[note 4]

Denmark

On 17 December 2013, Denmark's Financial Supervisory Authority (FSA) has issued a statement that echoes EBA's warning. In addition, FSA says that doing business with bitcoin does not fall under its regulatory authority and therefore FSA does not currently prevent anyone from opening such businesses.[57] FSA's chief legal adviser says that Denmark might consider amending existing financial legislation to cover virtual currencies.[58]

Ecuador

The National Assembly of Ecuador banned bitcoins including other decentralized digital/crypto currencies. Due to the establishment of a new state-run electronic money system. Ecuador's new project would be controlled by the government and tied directly to the local currency—the dollar. Users will be able to pay for select services and send money between individuals. This will begin in mid-February 2015. "Electronic money is designed to operate and support the monetary scheme of dollarization," economist Diego Martinez, a delegate of the President of the Republic to the Board of Regulation and Monetary and Financial Policy.[59]

Estonia

The Estonian Central bank refers to bitcoin as a "problematic scheme" and "Ponzi scheme".[60] The Estonian Financial Intelligence Unit stated that every person who exchanges any amount of bitcoin requires a license and that every person who trades more than 1000 Euro per months needs to be met in person and a copy of id made and kept.[61]

European Union

According to the European Central Bank, traditional financial sector regulation is not applicable to bitcoin because it does not involve traditional financial actors.[62]:5 Others in the EU have stated, however, that existing rules can be extended to include bitcoin and bitcoin companies.[10]

The European Central Bank classifies bitcoin as a convertible decentralized virtual currency.[62]:6 In July 2014 the European Banking Authority advised European banks not to deal in virtual currencies such as bitcoin until a regulatory regime was in place.[63]

In October 2015, the European Court of Justice ruled that bitcoin transactions are exempt from consumption tax similarly as traditional cash.[64] According to judges, the tax shouldn't be charged because bitcoins should be treated as a means of payment.[65]

Finland

Ruling 034/2014 by the Finnish Central Board of Taxes (CBT) stated that commission fees charged on bitcoin purchases by an exchange market were, under the EU VAT Directive, banking services and therefore VAT exempt. This is because the court classified bitcoins as payment instruments - whereas most countries treat their use as an unregulated method for the exchange of goods, or even as a crime.[66]

France

The French Ministry of Finance issued regulations on July 11, 2014 requiring:[14]

1) Identity verification during the opening of, withdrawal from, or deposit to a virtual currency account.

2) Capital gains are taxable as business profits (BIC) or as non-commercial profits (BNC), depending on if the activity is undertaken habitually or not. Assets held in bitcoin must also be reported pertaining to the wealth tax (ISF).

3) Proposed ceiling on payments consistent with current rules for cash payments.

4) Conformance with regulations at the European Union level for bitcoin exchanges pertaining to identity verification of transaction participants and anti-money laundering.

G7

In 2013 the G7's Financial Action Task Force issued the following statement in guidelines which may be applicable to companies involved in transmitting bitcoin and other currencies, "Internet-based payment services that allow third party funding from anonymous sources may face an increased risk of [money laundering/terrorist financing]." They concluded that this may "pose challenges to countries in [anti-money laundering/counter terrorist financing] regulation and supervision".[15]

Germany

On 19 August 2013, the German Finance Ministry announced that bitcoin is now essentially a "unit of account" and can be used for the purpose of tax and trading in the country. It is not classified as a foreign currency or e–money but stands as "private money" which can be used in "multilateral clearing circles", according to the ministry.[67]

Hong Kong

On 16 November 2013, Norman Chan, the chief executive of Hong Kong Monetary Authority (HKMA) said that bitcoins is only a virtual commodity. He also decided that bitcoins will not be regulated by HKMA. However, the authority will be closely watching the usage of bitcoins locally and its development overseas.[68]

Iceland

The Icelandic Central Bank confirmed that "it is prohibited to engage in foreign exchange trading with the electronic currency bitcoin, according to the Icelandic Foreign Exchange Act".[69]

India

In June 2013, the Reserve Bank of India (RBI) issued a notice acknowledging that virtual currencies posed legal, regulatory and operational challenges.[70] In August 2013, a spokesperson wrote in an email that bitcoin was under observation.[71]

On 24 December 2013, the Reserve Bank of India issued an advisory to the Indian public to be cautious in buying or selling of virtual currencies, including bitcoin.[72][73] Following the announcement bitcoin operators in the country began suspending operations.[74]

The first raid in India was undertaken a couple of days later in Ahmedabad by the Enforcement Directorate (ED) on the office of the website, buysellbit.co.in, that provided a platform to trade in this virtual currency. The preliminary investigations found it to be in violation of the Foreign Exchange Management Act (FEMA).[75]

On 28 December 2013, the Deputy Governor of the RBI, K. C. Chakrabarty, made a statement that RBI had no plans to regulate bitcoin.[19][76]

Indonesia

On 21 December 2013, Difi Ahmad, the executive director of communication at Bank Indonesia (BI) said that bitcoin is a potential payment method but could potentially be used in scams and money laundering operations. Since it is not regulated by banks, it has its associated risks. The central bank of Indonesia is currently studying bitcoin and they have no plans to issue regulations on it.[77]

On 16 January 2014, Ronald Waas, deputy governor of Bank Indonesia said that bitcoin usage would break a number of laws including *Undang-undang Bank Indonesia* (Bank Indonesia Act), *Undang-undang Informasi dan Transaksi Elektronik* (Information and Electronic Transaction Act), and *Undang-undang Mata Uang* (Monetary Act). For example, *Undang-undang Mata Uang* states that Rupiah is the only legal tender in the country. He also strongly advised the public against using bitcoins because security of bitcoins transactions are not guaranteed. However, currently BI does not have detailed policies of regulating or banning bitcoins usage.[78][79]

On 6 February 2014, Bank Indonesia is stating that bitcoin and other virtual currencies are not currencies or legal tender in Indonesia. The people are urged to exercise caution towards bitcoin and other virtual currencies. All risks regarding ownership or use of bitcoin are borne by the owner or user of bitcoin and other virtual currencies.[20][80] In September 2014, deputy governor of BI discourage the public against using bitcoin as a payment method.[81]

Israel

On February 19, 2014, the Bank of Israel issued a public service announcement detailing some of the risks associated with using bitcoin.[82]

On August 11, 2014, the Bank of Israel announced the formation of an inter-bureau team exploring the bitcoin issue, including representatives of the Bank of Israel, Ministry of Finance, Israel Money Laundering and Terror Financing Prohibition Authority, Israel Tax Authority, Israel Securities Authority and more. As of March 2015, no official guidelines regarding bitcoin have been published.[83]

The Israel Bar Association considers the virtual currency an appropriate form of payment for attorneys.[84]

Japan

On 7 March 2014, the Japanese government, in response to a series of questions asked in the National Diet, made a cabinet decision on the legal treatment of bitcoins in the form of answers to the questions.[85] The decision did not see bitcoin as currency nor bond under the current Banking Act and Financial Instruments and Exchange Law, prohibiting banks and securities companies from dealing in bitcoins. The decision also acknowledges that there are no laws to unconditionally prohibit individuals or legal entities from receiving bitcoins in exchange for goods or services. Taxes may be applicable to bitcoins.

According to *Nikkei Asian Review*, in February 2016, "Japanese financial regulators have proposed handling virtual currencies as methods of payment equivalent to conventional currencies".[86]

Jordan

The Central Bank of Jordan prohibits banks, currency exchanges, financial companies, and payment service companies from dealing in bitcoins or other digital currencies.[87] While it warned the public of risks of bitcoins, and that they are not legal tender, bitcoins are still accepted by small businesses and merchants.[87]

Lithuania

Bank of Lithuania released a warning on 31 January 2014 that bitcoin is not recognized as legal tender in Lithuania and that bitcoin users should be aware of high risks that come with the usage of it.[24]

Luxembourg

The Commission de Surveillance du Secteur Financier (CSSF) issued a communication in February 2014 stating the country's position regarding "virtual currencies":[25] "virtual" currencies are considered as money, since they are accepted as a means of payment of goods and services by a sufficiently large group of people.

More specifically, they are scriptural money as opposed to cash in the form of banknotes and coins. The scriptural nature does not require a tangible writing, similarly to electronic documents or signatures that do not require paper. Virtual currencies may thus be electronic money, but not necessarily within the meaning of the European Directive 2009/110 which provides for a definition of electronic money limited to its own scope.

The issuing of virtual currencies is not regulated from a monetary point of view. On the other hand, the CSSF reminds that nobody can be established in Luxembourg to carry out an activity of the financial sector without an authorisation by the Minister of Finance and without being subject to the prudential supervision of the CSSF (Article 14 of the law of 5 April 1993 on the financial sector).

Therefore, the potential interested persons who would like to establish themselves in Luxembourg in order to carry out an activity of the financial sector (as, for instance, the issuing of means of payments in the form of virtual or other currencies, the provision of payment services using virtual or other currencies, the creation of a market (platform) to trade virtual or other currencies) shall define their business purpose and their activity in a sufficiently concrete and precise manner to allow the CSSF to determine for which status they need to receive the ministerial authorisation.

The CSSF encouraged these individuals to contact its officials about facilitating digital currency-related commerce in the country, and suggested it will operate on a case-by-case basis with its regulatory decisions.[26]

The first Luxembourg "BitLicence" has been granted on 12 October 2015 to SnapSwap.[27] The CSSF explained in May 2015 that a few companies were in the process of acquiring a similar licences, further adding it was possible to get "Your licence within six months".[88]

Malaysia

On 4 November 2013, Bank Negara Malaysia (BNM) met with local bitcoin proponents to learn more about the currency but did not comment at the time.[89] BNM issued a statement on 6 January 2014 that bitcoin is not recognised as a legal tender in Malaysia. The central bank will not regulate bitcoin operations at the moment and users should aware of the risks associated with bitcoin usage.[90][91]

Norway

The Norwegian Tax Administration stated in December 2013 that they don't define bitcoin as money but regard it as an asset. Profits are subjected to wealth tax. In business, use of bitcoin falls under the sales tax regulation.[92]

Philippines

On 6 March 2014, Bangko Sentral ng Pilipinas (BSP) issued a statement on risks associated with bitcoin trading and usage. Bitcoin exchanges are not regulated by BSP at the moment. BSP will be monitoring the possibility of bitcoin usage in money laundering and other illegal purposes.[30]

Poland

Szymon Woźniak of the Ministry of Finance made an official announcement on the legality of bitcoin on 18 December 2013 at a conference at the Warsaw School of Economics stating that the Ministry of Finance does not consider bitcoin illegal and does not want to hinder its development.[93] He clarified that while not illegal, bitcoin cannot be considered legal tender, and, in the light of the directives of the European Union, it is neither electronic money.[93] As of January 27, 2015 several banks have closed accounts of clients trading bitcoin, and indicated “presumption of criminal offense” as the cause, with “criminal offense” presumably being “cryptocurrency trade”.[94]

Russia

CNBC reported that bitcoin was illegal in Russia in 2014,[33] as did the European Parliament.[10]:Russia Various Russian authorities and organizations have spoken out or taken actions against bitcoin. In early 2015, Russia’s media regulator blocked several bitcoin-related websites,[32] and a Russian state-owned media outlet reported that according to “the [Russian] Central Bank... bitcoin usage [is] illegal under Russian federal law,”[32] and in February 2014, the Russian Prosecutor General’s Office was quoted as saying, “Cyber currencies... including the most well-known, bitcoin, are money substitutes and cannot be used by individuals or legal entities.”[34] In 2014 the Bank of Russia issued a statement on bitcoin usage in which it was characterized as money substitute banned in Russia.[95] In February 2014, Russia’s Prosecutor General’s Office claimed that bitcoin is a money substitute and “cannot be used by individuals or legal entities”.[96] In September 2014, Deputy Finance Minister Aleksey Moiseev announced that a law will be passed by Spring 2015.[97] In July 2016, Deputy Finance Minister Aleksey Moiseev announced that the new law will define bitcoin as a foreign currency. Russians will be able to buy bitcoins and use them abroad. He is also expected that the new law will pass by the end of 2016.[98]

Singapore

On September 22, 2013, the Monetary Authority of Singapore (MAS) warned users of the risks associated with using bitcoin stating “If bitcoin ceases to operate, there may not be an identifiable party responsible for refunding their monies or for them to seek recourse”[99] and in December 2013 stated “Whether or not businesses accept bitcoins in exchange for their goods and services is a commercial decision in which MAS does not intervene”[100] In January 2014, the Inland Revenue Authority of Singapore issued a series of tax guidelines according to which bitcoin transactions may be treated as a barter exchange if it is used as a payment method for real goods and services. Businesses that deal with bitcoin currency exchanges will be taxed based on their bitcoin sales.[101]

Slovenia

On December 23, 2013 the Slovenian Ministry of Finance made an announcement [102] stating that bitcoin is neither a currency nor an asset. There is no capital gains tax chargeable on bitcoin, however bitcoin mining is taxed and businesses selling goods/services in bitcoin are also taxed.

Slovakia

The National Bank of Slovakia (NBS), stated[35] that bitcoin does not have the legal attributes of a currency, and therefore does not fall under national control.[note 5] European legislation, including the Slovak law, does not define the activities associated with virtual currency. Such activities are not regulated and supervised by the National Bank of Slovakia or the European Central Bank. At the same time NBS points out that any legal person or natural person in the Slovak Republic shall not issue any notes or any other coins. Unlawful manufacturing of banknotes and coins and putting them into circulation is punishable by law. In this context, NBS points out that virtual currencies have not a physical counterpart in the form of legal tender and participation in such a scheme (virtual currency) is at your own risk. Exchanges or purchases of virtual currencies represent the business risk of investors and investors' money are not protected. For any compensation or losses caused by such exchanges or purchases there is no legal entitlement.

South Africa

The South Africa Reserve Bank Position Paper on Virtual Currencies issued on 3 December 2014 came to 3 conclusions:[103]

1. The Bank does not oversee, supervise or regulate the Virtual Currency (VC) landscape, systems or intermediaries for effectiveness, soundness, integrity or robustness. Consequently, any and all activities related to the acquisition, trading or use of VCs (particularly Decentralized Convertible Virtual Currencies - DCVCs) are performed at the end-user‟s sole and independent risk and have no recourse to the Bank.

2. Given the current landscape and information currently available, the Bank contends that VCs pose no significant risk to financial stability, price stability or the National Payment System. However, end-users, whether individuals or businesses that accept VCs and businesses involved in the VCs ecosystem, are cautioned that any activities performed or undertaken with VCs are at their sole and independent risk.

3. In line with the Bank‟s position that regulation should follow innovation, the Bank continues monitoring developments in this regard and reserves the right to change its position should the landscape warrant regulatory intervention.

South Korea

There are no laws in South Korea regulating the use of bitcoin at present.[1]:South Korea On December 12, 2013, the president of the Bank of Korea recommended at a press conference that bitcoin be regulated in the future.[104]

Sweden

The Swedish jurisdiction is in general quite favorable for bitcoin businesses and users as compared to other countries within the EU and the rest of the world. The governmental regulatory and supervisory body Swedish Financial Supervisory Authority (Finansinspektionen) have legitimized the fast growing industry by publicly proclaiming bitcoin and other digital currencies as a means of payment. For certain businesses interacting with fiat (mainly exchanges) the current regulation dictates that an application for approval/license must be filed and all the AML/CTF and KYC regulations applicable to more traditional financial service providers must be followed.

Switzerland

On 5 December 2013 a proposal was put forth by 45 members of the Swiss Parliament for digital sustainability (Pardigli), that calls on the Swiss government to evaluate the opportunities for utilization of bitcoin by the country's financial sector.[105] It also seeks clarification on the bitcoin's legal standing with respect to VAT, securities and anti-money laundering laws.[106]

In response to the parliament postulates, the Swiss Federal Council issued a report on virtual currencies in June 2014.[107] The report states that since virtual currencies are not in a legal vacuum, the Federal Council has concluded that there is no need for legislative measures to be taken at the moment.

Taiwan

While bitcoin itself is not illegal here, approvals for bitcoin ATMs have been refused.[1]:Taiwan

On 6 December 2013, Perng Fai-nan said that bitcoin is only used in certain communities. Besides, he also opined that the value of bitcoin is a bubble and is highly volatile. Therefore, he advised the public against the speculation of bitcoins to prevent making a loss during the process. The central bank is closely watching the development of bitcoin and plan to impose regulations in the future.[108]

On 31 December 2013, Financial Supervisory Commission (Republic of China) (FSC) and CBC issued a joint statement which warns against the use of bitcoins. It is stated that bitcoins remains highly volatile, highly speculative, and is not entitled to legal claims or guarantee of conversion.[109]

On 5 January 2014, FSC chairman Tseng Ming-chung stated that FSC will not allow the installation of bitcoin ATM in Taiwan because bitcoin is not a currency and it should not be accepted by individuals and banks as payment.[110]

However, despite this, three of the four major convenience store chains in Taiwan make available bitcoin purchases through their kiosk systems,[111] and the largest chain now allows bitcoin to be used for purchases.[112]

Thailand

In 2013, the Thai monetary authority, the Bank of Thailand, "issued a preliminary ruling that using bitcoins as described was illegal."[43] A bitcoin startup denied a business license was reportedly told that "buying and selling bitcoins, using bitcoins to buy or sell goods and services, and transferring bitcoins in and out of Thailand were all currently illegal."[43]

Turkey

Bitcoin is not regulated as it is not considered to be electronic money according to the law.[1]:Turkey[113]

United Kingdom

Bitcoin is treated as 'private money'. When bitcoin is exchanged for sterling or for foreign currencies, such as euro or dollar, no VAT will be due on the value of the bitcoins themselves. However, in all instances, VAT will be due in the normal way from suppliers of any goods or services sold in exchange for bitcoin or other similar cryptocurrency. Profits and losses on cryptocurrencies are subject to capital gains tax.[114]

United States

The U.S. Treasury classified bitcoin as a convertible decentralized virtual currency in 2013.[45] A Magistrate Judge of a Texas U.S. District Court classified bitcoin as a currency.[115] A June 2014 U.S. government auction of almost 30,000 bitcoins, which the U.S. Marshals Service seized in October 2013 from Silk Road, was said to increase legitimacy of the currency.[116]

The U.S. Government Accountability Office (GAO) recommended in May 2013, that the Internal Revenue Service (IRS) formulate a tax guidance for bitcoin businesses.[117] End of March 2014, in time for 2013 tax filing, the IRS issued a guidance that it considered virtual currency as property for federal taxation and that “an individual who 'mines’ virtual currency as a trade or business [is] subject to self-employment tax”.[118]

In November 2013, the United States Senate held a committee hearing titled “Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies” to discuss virtual currencies.[119] At this hearing, held by senator Tom Carper, bitcoin and other currencies were received generally positively, in that bitcoin was a “legal means of exchange” and that “online payment systems, both centralized and decentralized, offer legitimate financial services” per US officials Peter Kadzik and Mythili Raman.[120][121]

The Federal Election Commission (FEC) deadlocked in November 2013 on whether to allow bitcoin in political campaigns with three Democrat members voting nay, three Republicans voting yea.[122] Political bitcoin pioneers New Hampshire House member Mark Warden[123] and Southern California politician Michael B. Glenn[124] independently from each other accepted bitcoin in their campaigns, and paved the way for others to follow suit. In May 2014, the FEC issued draft guidance to U.S. politicians who want to receive bitcoin donations.[125] It declined to declare bitcoins currency, stating they fit into its “anything of value” definition.[126]

In May 2014, Brett Stapper, co-founder of Falcon Global Capital, registered to lobby members of Congress and federal agencies on issues related to bitcoin.[127]

In January 2014, the U.S. Securities and Exchange Commission (SEC) focused on whether bitcoin-denominated stock exchanges were illegal, and inquired into unregistered securities offerings of the gambling site SatoshiDice and FeedZeBirds.[128] In May it warned investors that “both fraudsters and promoters of high-risk investment schemes may target bitcoin users”.[129] The SEC charged and settled with the former owner of SatoshiDice and FeedZeBirds in June 2014 for selling unregistered securities.[130] In October 2014, former SEC Chair Arthur Levitt joined BitPay, a bitcoin payment processor, and Vaurum, a bitcoin exchange for institutional investors in advisory roles.[131]

The U.S. Commodity Futures Trading Commission (CFTC) stated in March 2014 it considered regulation of digital currencies[132] after TeraExchange announced to launch a swap. TeraExchange constructed an index for the value of bitcoin from six different exchanges. The dollar value of a given bitcoin amount is locked in the swap. The CFTC approved the financial product in September 2014, satisfied it “could not easily be manipulated”.[133] There may be significant legal issues around security interests in bitcoin[134] under the Uniform Commercial Code.

In June 2014 California Assemblyman Roger Dickinson (D–Sacramento) submitted draft legislation (Assembly Bill 129) to legalize bitcoin and other forms of alternative and digital currency.[135][136] After the GAO had called for increased oversight of bitcoin, the Consumer Financial Protection Bureau warned consumers of bitcoin being risky.[137]

As of May 2015, New York state is the only state with a final bitcoin rule, commonly referred to as a BitLicense.[138] In March 2014, the New York State Department of Financial Services led by superintendent Benjamin Lawsky had officially invited bitcoin exchanges to apply with them,[139] and in July 2014 it published draft regulations for virtual currency businesses.[140] Businesses would have to provide transaction receipts, disclosures about risks, policies to handle customer complaints, maintain a cybersecurity program, hire a compliance officer and verify details about their customers to follow anti-money-laundering rules, per FinCEN.[140]

1.3.3 Footnotes

[1] Translated from: Podle § 6 odst. 1 AML zákona je za podezřelý obchod třeba považovat „obchod uskutečněný za okolností vyvolávajících podezření ze snahy o legalizaci výnosů z trestné činnosti nebo podezření, že v obchodu užité prostředky jsou určeny k financování terorismu“. FAÚ proto vyzývá všechny povinné osoby, aby v souvislosti s nákupem/prodejem jakékoli digitální měny, jako je například Bitcoin, byla jako velmi riziková k

posouzení a k rozhodnutí o dalších opatřeních podle okolností každá platba nad hodnotu 1.000 EUR a vždy jako podezřelý obchod postupem podle § 18 AML zákona oznámena transakce nad hodnotu 15.000 EUR.

[2] Translated from: Data evidovaná v protokolu bitcoin... nemají charakter pohledávky držitele bitcoinů za jinou osobou, nejsou to tedy bezhotovostní peněžní prostředky ani elektronické peníze (§ 4 ZPS), resp. peněžní prostředky ve smyslu ustanovení § 2 odst. 1 písm. c) ZPS. Nákup či prodej bitcoinů na vlastní účet nepředstavuje žádnou z platebních služeb podle § 3 odst. 1 ZPS ani bezhotovostní obchod s cizí měnou [§ 2 odst. 1 písm. e) ZPS]. Stejně tak nepředstavuje žádnou platební službu ve smyslu ZPS provedení transakce v rámci protokolu bitcoin (např. zaslání určitého množství bitcoinů jinému uživateli protokolu) ani "vedení účtu v bitcoinech" (kdy za vlastníka bitcoinů spravuje jeho bitcoiny, typicky v rámci "virtuální peněženky" na internetové stránce, jiná osoba)... Obchodování s bitcoiny proto nevyžaduje povolení ČNB (takové povolení ČNB ani nemůže udělit) a nepodléhá dohledu ČNB.

[3] Translated from: Samotný nákup a prodej bitcoinů statut povinné osoby nezakládá, ale pokud se některá povinná osoba – finanční instituce, obchodník s nemovitostmi či kulturními památkami, provozovatel loterie aj. – v rámci své podnikatelské činnosti setká s obchody s bitcoiny, měla by jim věnovat zvýšenou pozornost...

[4] Translated from: Závěrem dodáváme, že povolení ČNB není potřebné ani k přijímání úhrad zboží a služeb prostřednictvím bitcoinů. Je však třeba upozornit, že soustavné odmítání tuzemských bankovek a mincí by mohlo naplnit znaky skutkové podstaty trestného činu ohrožování oběhu tuzemských peněz.

[5] Translated from: ...bitcoin nespĺňa atribúty meny v právnom zmysle (jeho platnosť na určitom území nie je mocensky ustanovená, právny poriadok neupravuje jej obeh ani ochranu), zastávame názor, že ho nie je možné označovať za menu.

1.3.4 References

[1] "Regulation of Bitcoin in Selected Jurisdictions". *loc.gov*. The Law Library of Congress, Global Legal Research Center. 2014. Retrieved 25 February 2015.

[2] Hartge-Hazelman, Bianca (December 13, 2013). "Glenn Stevens says Bitcoins show promise, but so did tulips". *JHT*. The Australian Financial Review. Retrieved September 21, 2014.

[3] AFP (15 Sep 2014). "Why Bangladesh will jail Bitcoin traders". *telegraph.co.uk*. The Telegraph. Retrieved 23 February 2015.

[4] "Resolución 044/2014" (PDF) (in Spanish). Retrieved 2014-06-20.

[5] Cuthbertson, Anthony (20 June 2014). "Cryptocurrency Round-Up: Bolivian Bitcoin Ban, iOS Apps & Dogecoin at McDonald's". *ibtimes.co.uk*. International Business Times. Retrieved 23 February 2015.

[6] "Busca de Normativos". *www3.bcb.gov.br*. Retrieved 2016-09-11.

[7] "Закон за платежните услуги и платежните системи". *loc.gov*. Държавен вестник. 2015. Retrieved 28 July 2015.

[8] Canada: Can You Take A Security Interest In Bitcoin?,*Mondaq*,May 14.2014.Wednewday 4:10PM EST,Ms M. Sandra Appel(A security Agreement for Bitcoin: Is it Possible?)

[9] Rubenfeld, Samuel (23 June 2014). "Canada Enacts Bitcoin Regulations". *Risk and Compliance Journal*. Wall Street Journal. Retrieved 24 February 2015.

[10] Szczepański, Marcin (November 2014). "Bitcoin: Market, economics and regulation" (PDF). *European Parliamentary Research Service*. Annex B: Bitcoin regulation or plans therefor in selected countries. Members' Research Service. p. 9. Retrieved 18 February 2015.

[11] "Riesgos de las operaciones realizadas con "Monedas Virtuales"". Superintendencia Financiera de Colombia. 26 March 2014. Retrieved 20 October 2015.

[12] "Obchodování s bitcoiny" (PDF). Czech National Bank. Retrieved 19 March 2015.

[13] Cuthbertson, Anthony (1 September 2014). "Ecuador Reveals National Digital Currency Plans Following Bitcoin Ban". *ibtimes.co.uk*. International Business Times. Retrieved 23 February 2015.

[14] "Réguler les monnaies virtuelles" (PDF). Ministre des Finances. Retrieved 6 June 2016.

[15] "Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services" (PDF). *Guidance for a risk-based approach*. Paris: Financial Action Task Force (FATF). June 2013. p. 47. Retrieved 6 March 2014.

[16] "Significant risk attached to use of virtual currency". *cb.is*. The Central Bank of Iceland. 19 March 2014. Retrieved 17 June 2015.

[17] Fidel Martinez and Rob Wile (23 September 2014). "U.S. hesitation is chasing Bitcoin to Europe". Retrieved 8 January 2015.

[18] Nathaniel Popper (21 December 2013). "Into the Bitcoin Mines". *Deal Book New York Times*. New Yotk Times Company. Retrieved 9 December 2014.

[19] "No move to regulate Bitcoins: RBI". *The Times of India*. 29 December 2013. Retrieved 29 December 2013.

[20] Jacobs, Peter (6 February 2014). "Statement of Bank Indonesia Related To Bitcoin and Other Virtual Currency". *Press Releases*. Bank of Indonesia. Retrieved 20 October 2015.

[21] Bitconnect.co. "Japan Officially Recognizes Bitcoin and Digital Currencies as Money - Bitconnect".

[22] Knutsen, Elise (24 Feb 2014). "Despite warnings, Bitcoin gains toehold in region". *dailystar.com.lb*. The Daily Star. Retrieved 17 June 2015. [In February of 2014] the Central Bank of Jordan issued a warning against the currency, becoming the second government in the region to do so after Lebanon.

[23] "Warning of the National Bank of the Kyrgyz Republic on the spread and use of the "virtual currency", in particular, bitcoins (bitcoin)". *nbkr.kg*. National Bank of the Kyrgyz Republic. 18 July 2014. Retrieved 23 February 2015.

[24] "Lietuvos bankas apsisprendė dėl bitkoinų". vz.lt. 31 January 2014. Retrieved 31 January 2014.

[25] "Communique virtual currencies" (PDF). Commission de Surveillance du Secteur Financier. Retrieved 15 October 2015.

[26] Rizzo, Pete. "Luxembourg Opens Dialogue with Bitcoin Businesses in New Statement". *Regulation*. CoinDesk. Retrieved 19 October 2015.

[27] "SnapSwap granted first bitLicense in Europe". *SnapSwap*. Retrieved 19 October 2015.

[28] Rizzo, Pete (12 October 2015). "Scorechain Raises $570k for European Bitcoin Compliance Solution". *Companies*. CoinDesk. Retrieved 19 October 2015.

[29] "Legality of bitcoin in Pakistan". 20 November 2015.

[30] "Warning Advisory on Virtual Currencies". Bangko Sentral ng Pilipinas. 6 March 2014. Retrieved 10 March 2014.

[31] "Banca Naţională a României". *www.bnr.ro*. Retrieved 2016-02-03.

[32] "Russian media watchdog blocks Bitcoin sites". *rt.com*. RT/Russia Today (Autonomous Nonprofit Organization "TV-Novosti"). 13 January 2015. Retrieved 23 February 2015.

[33] Clinch, Matt (17 Dec 2014). "Russians move into bitcoin as ruble tanks". *cnbc.com*. CNBC. Retrieved 23 February 2015. A cryptocurrency exchange based in Bulgaria, called BTC-e, is known in the industry as being the most Russian-friendly despite bitcoin being made illegal in Russia.

[34] Baczynska, Gabriela (9 February 2014). "Russian authorities say Bitcoin illegal". *reuters.com*. Thompson Reuters. Retrieved 25 February 2015.

[35] "Niekoľko úvah k virtuálnej mene bitcoin" (PDF). Slovak National Bank. Retrieved 24 March 2015.

[36] "Position Paper on Virtual Currencies" (PDF). *South African Reserve Bank*.

[37] Russell, Jon (10 December 2013). "Korea becomes the latest Asian country to reject Bitcoin as a legitimate currency". *thenextweb.com*. The Next Web. Retrieved 26 February 2015.

[38] "Korean-American caught buying illegal drugs with Bitcoin". *The Korea Herald*. Herald Corporation. 17 March 2014. Retrieved 26 February 2015.

[39] "Fact sheet Status: Bitcoins" (PDF). *finma.ch/*. FINMA: Swiss Financial Market Supervisory Authority. 25 June 2014. Retrieved 26 February 2015. The use of bitcoins as a means of paying for goods and services in Switzerland is not regulated

[40] Reynolds, Sam. "BITCOIN NOW FOR SALE AT TAIWAN'S FAMILY MART". *vrworld.com*. VR World Media Hong Kong Ltd. Retrieved 9 July 2015.

[41] Horwitz, Josh (Oct 28, 2014). "Now you can buy bitcoin along with your snacks and sodas in 3,000 Taiwanese convenience stores". *techinasia.com*. Tech in Asia. Retrieved 8 July 2015. Sound complicated? It is. ... As you can see, it's best suited for folks who have already passed Bitcoin 101.

[42] Sangwongwanich, Pathom (18 Aug 2014). "Bitcoin firm licensed to trade in baht". *bangkokpost.com*. Bangkok Post. Retrieved 24 February 2015. Another bitcoin trading company has emerged as a legally registered entity in Thailand... despite doubts over the legality of the virtual currency.

[43] Watts, Jake Maxwell (31 July 2013). "Thailand's Bitcoin ban is not quite what it seems". *Quartz*. Atlantic Media. Retrieved 2 June 2015.

[44] "Bank of Thailand Says Bitcoin 'Not Illegal' But Warns Against its Use". *CoinDesk*. 2014-03-18. Retrieved 2016-05-10.

[45] "Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy". *fincen.gov*. Financial Crimes Enforcement Network. 19 November 2013. Retrieved 1 June 2014.

[46] "Press release on bitcoins and other virtual currencies". *SBV*. State Bank of Vietnam. 28 February 2014. Retrieved 28 November 2015.

[47] Han, Esher (21 August 2014). "Australian Tax Office decides bitcoins are assets, not currency". *The Sydney Morning Herald*. Retrieved 20 August 2015.

[48] "Tax treatment of crypto-currencies in Australia – specifically bitcoin". Australian Taxation Office (ATO). August 20, 2014. Retrieved October 12, 2014. and "Bitcoin for businesses". Australian Government. Retrieved October 12, 2014.

[49] "Tax treatment of crypto-currencies in Australia – specifically bitcoin". Australian Taxation Office (ATO). August 20, 2014. Retrieved October 12, 2014.

[50] "Bitcoin for businesses". Australian Government. Retrieved October 12, 2014.

[51] "China Bans Financial Companies From Bitcoin Transactions". Bloomberg. 5 December 2013. Retrieved 16 December 2013.

[52] “Bitcoin’s Outlook In China Is Not Looking So Good Right Now”. Business Insider. 16 December 2013. Retrieved 16 December 2013.

[53] “China Bitcoin Exchange CEO: We're Not Giving Up Yet”. 19 December 2013. Retrieved 19 December 2013.

[54] Chao Deng; Lingling Wei (1 April 2014). “China Cracks Down on Bitcoin”. *WSJ.com*. Dow Jones & Company. Retrieved 8 November 2014.

[55] Kelion, Leo (18 December 2013). “Bitcoin sinks after China restricts yuan exchanges”. *Technology*. BBC. Retrieved 22 October 2015.

[56] “Metodický pokyn o přístupu povinných osob k digitálním měnám”. MFCR. 25 September 2013. Retrieved 16 October 2015.

[57] “Advarsel mod virtuelle valutaer” [Warning against virtual currencies] (in Danish). Financial Supervisory Authority. December 17, 2013. Archived from the original on December 17, 2013.

[58] Schwartzkopff, Frances. “Bitcoins Spark Regulatory Crackdown as Denmark Drafts Rules”. Retrieved 24 December 2013.

[59] Martínez Vinueza, Diego; Rivera, Patrícío. “DBCE-0360-2013” (PDF). Banco Central del Ecuador. Retrieved 22 October 2015.

[60] Ummelas, Ott; Seputyte, Milda (31 January 2014). “Bitcoin 'Ponzi' Concern Sparks Warning From Estonia Bank”. *BloombergBusiness*. Bloomberg. Retrieved 22 October 2015.

[61] Rahapesu andmebüroo juht Aivar Paul bitcoinidega seonduvast, politsei.ee

[62] European Central Bank (October 2012). *Virtual Currency Schemes* (PDF). Frankfurt am Main: European Central Bank. ISBN 978-92-899-0862-7. Retrieved 5 March 2014.

[63] “EBA Opinion on 'virtual currencies” (pdf). European Banking Authority. 4 July 2014. p. 46. Retrieved 8 July 2014.

[64] “Bitcoin currency exchange not liable for VAT taxes: top EU court”. *Reuters*. 22 October 2015. Retrieved 23 October 2015.

[65] Bodoni, Stephanie; Thomson, Amy (22 October 2015). “EU’s Top Court Rules That Bitcoin Exchange Is Tax-Free”. *BloombergBusiness*. Bloomberg. Retrieved 23 October 2015.

[66] Joe Stanley-Smith (14 November 2014). “Finland recognises Bitcoin services as VAT exempt”. International Tax Review. Retrieved 15 November 2014.

[67] Clinch, Matt (19 August 2013). “Bitcoin recognized by Germany as 'private money'". CNBC. Retrieved 18 January 2014.

[68] "⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰ (Bitcoin is not regulated by HKMA)". Ta Kung Pao. 16 November 2013. Retrieved 18 January 2014.

[69] “Höftin stöðva viðskipti með Bitcoin (Controls suspend trading in bitcoin)". *mbl.is* (in Icelandic). Morgunblaðsins. 19 December 2013. Retrieved 19 December 2013.

[70] “RBI red flags 'virtual currency'". The Times of India. June 28, 2013. Retrieved September 15, 2014.

[71] “Reserve Bank of India won't regulate virtual currency Bitcoin, yet”. *The Economic Times*. 14 August 2013. Retrieved 29 December 2013.

[72] “RBI cautions users of Virtual Currencies against Risks”. Reserve Bank of India. December 24, 2013. Retrieved September 15, 2014.

[73] “Reserve Bank warns against Bitcoin use”. *The Hindu*. 24 December 2013. Retrieved 29 December 2013.

[74] “Bitcoin operators shut shop in India amid RBI warning”. *The Economic Times*. 27 December 2013. Retrieved 29 December 2013.

[75] “First time in the country, ED raids a Bitcoin seller in Ahmedabad”. *DNA India*. 27 December 2013. Retrieved 29 December 2013.

[76] "'RBI neither regulates nor supports bitcoins'". *The Hindu Business Line*. 28 December 2013. Retrieved 29 December 2013.

[77] Baskoro, FM (21 December 2013). “Bitcoin Finds Itty-Bitty Market in Indonesia”. Jakarta Globe. Retrieved 18 January 2014.

[78] Ryan, Huang (20 January 2014). “Indonesia warns against Bitcoin usage - The central bank said the digital currency was not covered under any regulations, and highlighted the risks involved in transaction security”. ZDNet. Archived from the original on 17 September 2015. Retrieved 15 October 2015.

[79] “BI: Pemakaian bitcoin melanggar Undang-undang! (BI: Bitcoin usage violates the law!)". KONTAN. 16 January 2014. Retrieved 15 October 2015.

[80] “Pernyataan Bank Indonesia Terkait Bitcoin dan Virtual Currency Lainnya (Bank Indonesia statement on bitcoin and other virtual currencies)". Bank Indonesia. 6 February 2014. Retrieved 7 February 2014.

[81] “BI Minta Publik Mewaspadai Transaksi Bitcoin (BI requested the public to be careful of Bitcoin transactions)". Tempo (Indonesian magazine). 5 September 2014. Retrieved 15 October 2015.

[82] "בנק ישראל - הודעות לעיתונות - הודעה לציבור בדבר סיכונים אפשריים הטמונים במטבעות וירטואליים מבוזרים (דוגמת ביטקוין)".

[83] "בנק ישראל - הודעות לעיתונות - צוות בין-משרדי בנושא מטבעות וירטואליים מבוזרים".

[84] “Government considers taxing Bitcoin profits”. 12 September 2013. Retrieved 26 December 2013.

[85] “The First Governmental View: Bitcoin is not Currency (in Japanese)". *Nikkei Inc*. 7 March 2014.

[86] "Japan eyes treating bitcoins the same as real money". *Nikkei Asian Review*. The Nikkei. 24 February 2016. Retrieved 28 April 2016.

[87] Obeidat, Omar (22 February 2014). "Central bank warns against using bitcoin". *The Jordan Times*.

[88] Labro, Thierry (22 May 2015). "Monnaies virtuelles: un agrément en six mois". Luxemburger Post. Retrieved 22 October 2015.

[89] "Bank Negara's Officially Unofficial Statement on Bitcoin is No Statement". Betanomics.asia. Retrieved September 21, 2014.

[90] "Statement on Bitcoin". Bank Negara Malaysia. 6 January 2014. Retrieved 2 March 2014.

[91] Fuad, Madiha (6 January 2014). "BNM warns on Bitcoin risks". The Edge (Malaysia). Retrieved 11 January 2014.

[92] Saleha Mohsin (13 December 2013) Bitcoins Fail Currency Test in Scandinavia's Richest Nation Bloomberg. Retrieved 13 December 2013

[93] "MinFin: Bitcoin nie jest nielegalny". Puls Biznesu. 18 December 2013. Retrieved 18 December 2013.

[94] "Banks closed current accounts for Bitcoin trade" (in Polish). bankier.pl. 27 January 2015. Retrieved 28 January 2015.

[95] Об использовании при совершении сделок "виртуальных валют", в частности, Биткойн (in Russian). Bank of Russia. 27 January 2014. Retrieved 10 March 2014.

[96] Hamburger, Ellis (February 9, 2014). "Russia bans Bitcoin use". *The Verge*. Retrieved February 10, 2014.

[97] "'You can play with you bitcoins, but you can't pay with them': Russia may ban cryptocurrencies by 2015". Russia Today. September 12, 2014.

[98] "ru:Биткоины переезжают за границу". ru:Российская Газета. July 18, 2016.

[99] Irene Tham (2013-09-22). "Bitcoin users beware: MAS | AsiaOne Business". Business.asiaone.com. Retrieved 2013-12-27.

[100] Terence Lee (2013-12-23). "Singapore government decides not to interfere with Bitcoin". Techinasia.com. Retrieved 2013-12-27.

[101] Tay, Liz (9 January 2014). "Singaporean Tax Authorities Have Issued Guidance On Bitcoin-Related Sales And Earnings". Business Insider (Australia). Retrieved 11 January 2014.

[102] "Davčna obravnava poslovanja z virtualno valuto po ZDoh-2 in ZDDPO-2 | Davčna uprava RS" (in Slovenian). Durs.gov.si. 2013-12-23. Retrieved 2013-12-27.

[103] "Position Paper on Virtual Currencies" (PDF). *South African Reserve Bank*.

[104] "□□ "□□ □□□□ □□ □□□□"" [Bank of Korea:"Government Needs to Make Bitcoin Regulation"]. HANKOOKI. December 27, 2013. Retrieved September 21, 2014.

[105] "Swiss Parliament: Rechtssicherheit für Bitcoin schaffen". Parlament.ch. Retrieved 2013-12-27.

[106] "Swiss Parliament: Bitcoin and AML". Parlament.ch. Retrieved 2014-04-16.

[107] "Federal Council report on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates" (PDF). *Federal Council (Switzerland)*. Swiss Confederation. 25 June 2014. Retrieved 28 November 2014.

[108] □□, □ (6 December 2013). "□□□□□□□□ □□□□□□□ □□□□□□ (Taiwan is not crazy about bitcoin. The central bank does not regulate it but the public is advised not to speculate on it)". China Times. Retrieved 18 January 2014.

[109] Crystal, Hsu (31 December 2013). "Regulators warn against using bitcoins". Taipei Times. Retrieved 15 October 2015.

[110] Shu, Catherine (5 January 2014). "Taiwan's Government Says No To Bitcoin ATMs". TechCrunch. Retrieved 18 January 2014.

[111] "FSC vows to keep hands off bitcoin management". Taipei Times. 19 November 2015.

[112] "FamilyMart Now Accpets BitoEX's Bitcoin Wallet to Buy Goods". Medium.com. 26 October 2015.

[113] "Press release" (PDF) (Press release). Turkish Banking Regulation and Supervision Agency. 25 November 2013.

[114] "Tax treatment of activities involving Bitcoin and other similar cryptocurrencies". HM Revenue & Customs.

[115] *SEC v. Trendon T. Shavers and Bitcoin Savings and Trust*, 416 (E.D. Tex. 2013).

[116] Alex Hern (1 July 2014). "Silk Road's legacy 30,000 bitcoin sold at auction to mystery buyers". The Guardian. Retrieved 31 October 2014.

[117] US Government Accountability Office (May 2013). "Virtual Economies and currencies: Additional IRS guidance could reduce tax compliance risks". *GAO Report GAO-13-516*. Report to the Committee on Finance, U.S. Senate. Retrieved 6 March 2014.

[118] IRS (25 March 2014). "IRS Virtual Currency Guidance" (PDF). *Notice 2014-21*. IRS. Retrieved 30 March 2014.

[119] Rushe, Dominic (18 November 2013). "Bitcoin hits $700 high as Senate stages hearing on virtual currency". *The Guardian*. Retrieved 24 November 2013.

[120] Raskin, Max (18 November 2013). "U.S. Agencies to Say Bitcoins Offer Legitimate Benefits". *Bloomberg*. Retrieved 24 November 2013.

[121] Lee, Timothy (23 November 2013). "For Bitcoin, a successful charm offensive on the Hill". *Washington Post*. Retrieved 24 November 2013.

[122] Gillum, Jack (2013-04-03). "FEC: Donors can't use bitcoins for contributions". Bigstory.ap.org. Retrieved 2013-12-27.

[123] "Donate to the campaign | Mark Warden — State Rep". Markwarden.com. Retrieved 9 November 2014.

[124] Foxhall, Emily (20 December 2013). "Bitcoin donations welcome, Newport Beach City Council candidate says". latimes.com. Retrieved 27 December 2013.

[125] Goodman, Lee E. (8 May 2014). "FEC Advisory Opinion 2014-02" (PDF). Federal Election Commission. Retrieved 8 May 2014.

[126] Levinthal, Dave (8 May 2014). "What the FEC's Bitcoin ruling means". *Center for Public Integrity*. Retrieved 8 May 2014.

[127] Hattem, Julian (23 May 2014). "Bitcoin gets a lobbyist". The Hill. Retrieved 27 May 2014.

[128] Dougherty, Carter (20 March 2014). "Gambling Website's Bitcoin-Denominated Stock Draws SEC Inquiry". *Bloomberg BusinessWeek.com*. Bloomberg LP. Retrieved 13 June 2014.

[129] "Investor Alert: Bitcoin and Other Virtual Currency-Related Investments". *Investor.gov*. U.S. Securities and Exchange Commission. Retrieved 13 May 2014.

[130] "Press Release SEC Charges Bitcoin Entrepreneur With Offering Unregistered Securities". SEC.gov. 3 June 2014. Retrieved 13 June 2014.

[131] Michael J. Casey (28 October 2014). "Ex-SEC Chairman Levitt to Advise Two Bitcoin Companies". *WSJ*. Retrieved 27 December 2014.

[132] Miedema, Douwe (11 March 2014). "U.S. swaps watchdog says considering bitcoin regulation". *Reuters.com*. Retrieved 11 March 2014.

[133] Douwe Miedema (12 September 2014). "Bitcoin gets boost as U.S. watchdog approves first swap". *Chicago Tribune*. Reuters. Retrieved 19 January 2015.

[134] Cowan, Miles. "Uniform Commercial Code and Bitcoin". *We Use Coins*. Retrieved 27 November 2014.

[135] Cosco, Joey (25 June 2014). "Bitcoin Is Actually Illegal In California, But That Could Change Soon". Business Insider. Retrieved 26 June 2014.

[136] "Bill Text - AB-129 Lawful money.". *leginfo.legislature.ca.gov*. Retrieved 2016-01-31.

[137] Peter Schroeder (11 August 2014). "CFPB warns consumers about bitcoin 'Wild West'". *The Hill*. News Communications, Inc. Retrieved 27 August 2014.

[138] Nathaniel Popper (7 May 2015). "Bitcoin Exchange Receives First License in New York State". *The New York Times*. Retrieved 11 May 2015.

[139] "In the Matter of Virtual Currency Exchanges" (PDF). *Public Order*. New York State Department of Financial Services. 11 March 2014. Retrieved 30 March 2014.

[140] Vigna, Paul (17 July 2014). "NY Financial Regulator Releases Draft of 'Bitlicense' for Bitcoin Businesses". *WSJ*. Dow Jones & Company.

Chapter 2

People

2.1 Satoshi Nakamoto

Satoshi Nakamoto is the name used by the person or people who designed bitcoin and created its original reference implementation, Bitcoin Core (formerly known as Bitcoin-Qt).[1]

2.1.1 Development of bitcoin

In October 2008, Nakamoto published a paper[2][3] on The Cryptography Mailing list at metzdowd.com[4] describing the bitcoin digital currency. In January 2009, Nakamoto released the first bitcoin software that launched the network and the first units of the bitcoin cryptocurrency, called *bitcoins*.[5][6]

Nakamoto continued to collaborate with other developers on the bitcoin software until mid-2010. Around this time, he handed over control of the source code repository and network alert key to Gavin Andresen,[7] transferred several related domains to various prominent members of the bitcoin community, and stopped his involvement in the project.

The public bitcoin transaction log shows that Nakamoto's known addresses contain roughly one million bitcoins.[8] As of 22 August 2016, this is the equivalent of US$581 million.[9]

2.1.2 Characteristics

On his P2P Foundation profile as of 2012, Nakamoto claimed to be a 37-year-old male who lived in Japan,[10] but some speculated he was unlikely to be Japanese due to his use of perfect English and his bitcoin software not being documented or labelled in Japanese.[11]

Occasional British English spelling and terminology (such as the phrase “bloody hard”) in both source code comments and forum postings led to speculation that Nakamoto, or at least one individual in the consortium claiming to be him, was of Commonwealth origin.[2][11][12]

Stefan Thomas, a Swiss coder and active community member, graphed the time stamps for each of Nakamoto's bitcoin forum posts (more than 500); the resulting chart showed a steep decline to almost no posts between the hours of 5 a.m. and 11 a.m. Greenwich Mean Time. Because this pattern held true even on Saturdays and Sundays, it suggested that Nakamoto was asleep at this time.[11] If Nakamoto is a single individual with conventional sleeping habits, it suggests he resided in a region using the UTC−05:00 or UTC−06:00 time offset. This includes the parts of North America that fall within the Eastern Time Zone and Central Time Zone, as well as parts of Central America, the Caribbean and South America.

2.1.3 Candidates

There is still doubt about the real identity of Satoshi Nakamoto, as the below information shows:

Nick Szabo

In December 2013, a blogger named Skye Grey linked Nick Szabo to the bitcoin's whitepaper using a stylometric analysis.[13][14][15] Szabo is a decentralized currency enthusiast and published a paper on “bit gold”, which is considered a precursor to bitcoin.[14][15] He is known to have been interested in using pseudonyms in the 1990s.[16] In a May 2011 article, Szabo stated about the bitcoin creator: “Myself, Wei Dai, and Hal Finney were the only people I know of who liked the idea (or in Dai's case his related idea) enough to pursue it to any significant extent until Nakamoto (assuming Nakamoto is not really Finney or Dai).”[17]

Detailed research by financial author Dominic Frisby provides much circumstantial evidence but, as he admits, no proof that Satoshi is Szabo.[18] Speaking on RT's *The Keiser Report*, he said “I've concluded there is only one person in the whole world that has the sheer breadth but also the specificity of knowledge and it is this chap ...”.[19] But Szabo has denied being Satoshi. In a July 2014 email to Frisby, he said: 'Thanks for letting me know. I'm afraid you got it wrong doxing me as Satoshi, but I'm used to it'.[20] Nathaniel Popper wrote in the *New York Times* that "the most convincing evidence pointed to a reclusive American man of Hungarian descent named Nick Szabo."[21]

Dorian Nakamoto

In a high-profile March 6, 2014, article in the magazine *Newsweek*,[22] journalist Leah McGrath Goodman identified Dorian Prentice Satoshi Nakamoto, a Japanese American man living in California, whose birth name is Satoshi Nakamoto,[22][23][24] as the Nakamoto in question. Besides his name, Goodman pointed to a number of facts that circumstantially suggested he was the bitcoin inventor.[22] Trained as a physicist, Nakamoto worked as a systems engineer on classified defense projects and computer engineer for technology and financial information services companies. Nakamoto was laid off twice in the early 1990s and turned libertarian, according to his daughter, and encouraged her to start her own business and "not be under the government's thumb." In the article's seemingly biggest piece of evidence, Goodman wrote that when she asked him about bitcoin during a brief in-person interview, Nakamoto seemed to confirm his identity as the bitcoin founder by stating: "I am no longer involved in that and I cannot discuss it. It's been turned over to other people. They are in charge of it now. I no longer have any connection."[22] (This quote was later confirmed by deputies at the Los Angeles County Sheriff's Department who were present at the time.)[25]

The article's publication led to a flurry of media interest, including reporters camping out near Dorian Nakamoto's house and briefly chasing him by car when he drove to an interview.[26] However, during the subsequent full-length interview, Dorian Nakamoto denied all connection to bitcoin, saying he had never heard of the currency before, and that he had misinterpreted Goodman's question as being about his previous work for military contractors, much of which was classified.[27] Later that day, the pseudonymous Nakamoto's P2P Foundation account posted its first message in five years, stating: "I am not Dorian Nakamoto."[28][29]

Hal Finney

Hal Finney (May 4, 1956 – August 28, 2014) was a pre-bitcoin cryptographic pioneer and the first person (other than Satoshi himself) to use the software, file bug reports, and make improvements.[30] He also lived a few blocks from Dorian Nakamoto's family home, according to *Forbes* journalist Andy Greenberg.[31] Greenberg asked the writing analysis consultancy Juola & Associates to compare a sample of Finney's writing to Satoshi Nakamoto's, and they found that it was the closest resemblance they had yet come across (including the candidates suggested by *Newsweek*, *Fast Company*, *The New Yorker*, Ted Nelson and Skye Grey).[31] Greenberg theorized that Finney may have been a ghostwriter on behalf of Nakamoto, or that he simply used his neighbor Dorian's identity as a "drop" or "patsy whose personal information is used to hide online exploits". However, after meeting Finney, seeing the emails between him and Satoshi, his bitcoin wallet's history including the very first bitcoin transaction (from Satoshi to him, which he forgot to pay back) and hearing his denial, Greenberg concluded Finney was telling the truth. Juola & Associates also found that Satoshi's emails to Finney more closely resemble Satoshi's other writings than Finney's do. Finney's fellow extropian and sometimes co-blogger Robin Hanson assigned a subjective probability of "at least" 15% that "Hal was more involved than he's said", before further evidence suggested that was not the case.[32]

Craig Steven Wright

On 8 December 2015, *Wired* wrote that Craig Steven Wright, an Australian former academic, "either invented bitcoin or is a brilliant hoaxer who very badly wants us to believe he did".[33] Craig Wright took down his Twitter account and neither he nor his ex-wife responded to press inquiries. The same day, Gizmodo published a story with evidence obtained by a hacker who supposedly broke into Wright's email accounts, claiming that Satoshi Nakamoto was a joint pseudonym for Craig Steven Wright and computer forensics analyst David Kleiman, who died in 2013.[34] A number of prominent bitcoin promoters remained unconvinced by the reports.[35] Subsequent reports also raised the possibility that the evidence provided was an elaborate hoax,[36][37] which *Wired* acknowledged "cast doubt" on their suggestion that Wright was Nakamoto.[38]

On 9 December, only hours after *Wired* claimed Wright was Nakamoto, Wright's home in Gordon, New South Wales was raided by at least ten police officers. His business premises in Ryde, New South Wales were also searched by police. The Australian Federal Police stated they conducted searches to assist the Australian Taxation Office and that "This matter is unrelated to recent media reporting regarding the digital currency bitcoin."[39] According to a document released by Gizmodo alleged to be a transcript of a meeting between Wright and the ATO, he had been involved in a taxation dispute with them for several years.[34]

On 2 May 2016, Craig Wright posted on his blog publicly claiming to be Satoshi Nakamoto. In articles released on the same day, journalists from the BBC and *The Economist* stated that they saw Wright signing a message using the private key associated with the first bitcoin transaction.[40][41] Wright's claim was supported by Jon Matonis (former director of the Bitcoin Foundation) and bitcoin developer Gavin Andresen, both of whom met Wright and witnessed a similar signing demonstration.[42]

However, bitcoin developer Peter Todd said that Wright's blog post, which appeared to contain cryptographic proof, actually contained nothing of the sort.[43] The Bitcoin Core project released a statement on Twitter saying “There is currently no publicly available cryptographic proof that anyone in particular is Bitcoin’s creator.”[44][45] Bitcoin developer Jeff Garzik agreed that evidence publicly provided by Wright does not prove anything, and security researcher Dan Kaminsky concluded Wright’s claim was “intentional scammery”.[46][47]

On May 4, Wright made another post on his blog promising to publish “a series of pieces that will lay the foundations for this extraordinary claim”.[48][49] But the following day, he deleted all his blog posts and replaced them with a notice entitled “I'm Sorry”, which read in part:

> I believed that I could put the years of anonymity and hiding behind me. But, as the events of this week unfolded and I prepared to publish the proof of access to the earliest keys, I broke. I do not have the courage. I cannot.[50][51]

In June 2016, the *London Review of Books* published a 35,000 word article by Andrew O'Hagan about the events, based on discussions with Wright and many of the other people involved.[52][53] It also reveals that the Canadian company nTrust was behind Wright’s claim made in May 2016.

Other speculation

- In a 2011 article in *The New Yorker*, Joshua Davis claimed to have narrowed down the identity of Nakamoto to a number of possible individuals, including the Finnish economic sociologist Dr. Vili Lehdonvirta and Irish student Michael Clear, then a graduate student in cryptography at Trinity College Dublin.[54] Clear strongly denied he was Nakamoto,[55] as did Lehdonvirta.[56]

- In October 2011, writing for *Fast Company*, investigative journalist Adam Penenberg cited circumstantial evidence suggesting Neal King, Vladimir Oksman and Charles Bry could be Nakamoto.[57] They jointly filed a patent application that contained the phrase “computationally impractical to reverse” in 2008, which was also used in the bitcoin white paper by Nakamoto.[58] The domain name bitcoin.org was registered three days after the patent was filed. All three men denied being Nakamoto when contacted by Penenberg.[57]

- In May 2013, Ted Nelson speculated that Nakamoto is really Japanese mathematician Shinichi Mochizuki.[59] Later, an article was published in *The Age* newspaper that claimed that Mochizuki denied these speculations, but without attributing a source for the denial.[60]

- A 2013 article,[61] in *Vice* listed Gavin Andresen, Jed McCaleb, or a government agency as possible candidates to be Nakamoto. Dustin D. Trammell, a Texas-based security researcher, was suggested as Nakamoto, but he publicly denied it.[62]

- In 2013, two Israeli mathematicians, Dorit Ron and Adi Shamir, published a paper claiming a link between Nakamoto and Ross William Ulbricht. The two based their suspicion on an analysis of the network of bitcoin transactions,[63] but later retracted their claim.[64]

Some considered Nakamoto might be a team of people; Dan Kaminsky, a security researcher who read the bitcoin code,[65] said that Nakamoto could either be a “team of people” or a “genius”;[12] Laszlo Hanyecz, a former bitcoin core developer who had emailed Nakamoto, had the feeling the code was too well designed for one person.[11]

2.1.4 References

[1] S., L. (2 November 2015). “Who is Satoshi Nakamoto?". *The Economist explains*. The Economist.

[2] Nakamoto, Satoshi (24 May 2009). “Bitcoin: A Peer-to-Peer Electronic Cash System” (PDF). Retrieved 5 March 2014.

[3] Nakamoto, Satoshi (31 October 2008). “Bitcoin P2P e-cash paper”. Retrieved 5 March 2014.

[4] “Satoshi’s posts to Cryptography mailing list”. Mail-archive.com. Retrieved 2013-12-14.

[5] Davis, Joshua. “The Crypto-Currency: Bitcoin and its mysterious inventor.”. *The New Yorker*.

[6] Penenberg, Adam. “The Bitcoin Crypto-Currency Mystery Reopened”. Fast Company. A New Yorker writer implies he found Bitcoin’s mysterious creator. We think he got the wrong man, and offer far more compelling evidence that points to someone else entirely.

[7] Bosker, Bianca. “Gavin Andresen, Bitcoin Architect: Meet The Man Bringing You Bitcoin (And Getting Paid In It)". HuffPostTech.

[8] McMillan, Robert (18 December 2013). “Who Owns the World’s Biggest Bitcoin Wallet? The FBI”. Wired. Retrieved 31 May 2016.

[9] “Bitcoin Currency Data”. *www.quandl.com*. Quandl. Retrieved 31 May 2016.

[10] “Satoshi Nakamoto’s Page”. *P2P Foundation*. Retrieved 2 May 2016.

[11] Wallace, Benjamin (23 November 2011). “The Rise and Fall of Bitcoin”. Wired. Retrieved 31 May 2016. It seemed doubtful that Nakamoto was even Japanese. His English had the flawless, idiomatic ring of a native speaker.

[12] Jeffries, Adrianne (4 October 2011). "The New Yorker's Joshua Davis Attempts to Identify Bitcoin Creator Satoshi Nakamoto". Betabeat. Retrieved 27 December 2013.

[13] John Biggs. "Who is the real Satoshi Nakamoto? One researcher may have found the answer". TechCrunch. Retrieved 2014-03-06.

[14] Grey, Skye (2013-12-01). "Satoshi Nakamoto is (probably) Nick Szabo". Retrieved 2014-03-13.

[15] Grey, Skye (2014-03-11). "Occam's Razor: who is most likely to be Satoshi Nakamoto?". Retrieved 2014-03-15.

[16] "Re: on anonymity, identity, reputation, and spoofing". 1993-10-18. Retrieved 2014-03-15.

[17] Nick Szabo (2011-05-28). "Bitcoin, what took ye so long?". Retrieved 2014-03-12.

[18] Frisby, Dominic (2014) "Who is Satoshi Nakamoto?" In Bitcoin : the Future of Money?, p 85-149. Unbound. ISBN 1783520779

[19] "Nick Szabo is (probably) Satoshi Nakamato". 2014-11-06. Retrieved 2014-11-06. at ~17:30 into the show

[20] Frisby p 147

[21] Popper, Nathaniel. "Decoding the Enigma". *New York Times*. the most convincing evidence pointed to a reclusive American man of Hungarian descent named Nick Szabo.

[22] Leah McGrath Goodman (6 March 2014). "The Face Behind Bitcoin". *Newsweek*. Retrieved 6 March 2014.

[23] Andy Greenberg. "Bitcoin Community Responds To Satoshi Nakamoto's Outing With Disbelief, Anger, Fascination". Forbes. Retrieved 2014-03-06.

[24] Oremus, Will (2013-11-26). "The real Satoshi Nakamoto: Newsweek finds mysterious bitcoin creator in Los Angeles". Slate.com. Retrieved 2014-03-06.

[25] Winton, Richard (2014-03-07). "Deputies: Newsweek Bitcoin story quoted Satoshi Nakamoto accurately". *Los Angeles Times*. Retrieved 2014-03-09.

[26] Rodriguez, Salvador (2014-03-06). "Dorian Satoshi Nakamoto chased by reporters, denies founding Bitcoin". *Los Angeles Times*. Retrieved 2014-03-06.

[27] Nakashima, Ryan. "Man said to create Bitcoin denies it". Associated Press. Retrieved 2014-03-07.

[28] "Bitcoin open source implementation of P2P currency". 2014-03-07. Retrieved 2014-03-07.

[29] "'Real' bitcoin creator: 'I am not Dorian Nakamoto'". CNBC.

[30] "Hal Finney received the first Bitcoin transaction. Here's how he describes it.". *Washington Post*. Retrieved 24 February 2015.

[31] Andy Greenberg (2014-03-25). "Nakamoto's Neighbor: My Hunt For Bitcoin's Creator Led To A Paralyzed Crypto Genius". *Forbes*. Retrieved 2016-01-18.

[32] "Conspiracy Theory, Up Close & Personal". 2014-03-25. Retrieved 2014-03-25.

[33] Greenberg, Andy; Branwen, Gwern (December 8, 2015). "Bitcoin's Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius". Wired. Retrieved December 8, 2015.

[34] Biddle, Sam; Cush, Andy (December 8, 2015). "This Australian Says He and His Dead Friend Invented Bitcoin". Gizmodo. Retrieved December 8, 2015.

[35] Kaminska, Izabella (9 December 2015). "So, Satoshi is an Aussie?". *FT Alphaville*. Retrieved 9 December 2015.

[36] Jeong, Sarah (9 December 2015). "Satoshi's PGP Keys Are Probably Backdated and Point to a Hoax". Motherboard. Retrieved 10 December 2015.

[37] Ryall, Jenni (10 December 2015). "New chase for Bitcoin founder leaves everyone exhausted and no wiser". *Mashable*. Mashable. Retrieved 10 December 2015.

[38] Greenberg A (11 December 2015). "New Clues Suggest Craig Wright, Suspected Bitcoin Creator, May Be a Hoaxer". *Wired*. Retrieved 12 December 2015.

[39] Hunt, Ellie; Farrell, Paul (9 December 2015). "Reported bitcoin 'founder' Craig Wright's home raided by Australian police". *The Guardian*. London. Retrieved 9 December 2015.

[40] "Creator of Bitcoin digital cash reveals identity - BBC News". *BBC News*. BBC. BBC. 2 May 2016. Retrieved 2 May 2016.

[41] "Craig Steven Wright claims to be Satoshi Nakamoto. Is he?". *The Economist*. 2 May 2016. Retrieved 2 May 2016.

[42] *Satoshi*, archived from the original on 2016-05-05, retrieved 2016-05-07

[43] Thomas Fox-Brewster (2 May 2016). "Craig Wright Claims He's Bitcoin Creator Satoshi -- Experts Fear An Epic Scam". *Forbes*.

[44] "Bitcoin Core Project". *Twitter*.

[45] http://www.investopedia.com/articles/insights/050216/has-bitcoin-creator-satoshi-nakamoto-been-found.asp

[46] "Craig Wright's New Evidence That He Is Satoshi Nakamoto Is Worthless". *Motherboard*.

[47] "Validating Satoshi (Or Not)". *Dan Kaminsky's Blog*.

[48] Alex Hern. "Bitcoin: Craig Wright promises new evidence to prove identity". *the Guardian*.

[49] *Extraordinary Claims Require Extraordinary Proof - Dr. Craig Wright BlogDr. Craig Wright Blog*, archived from the original on 2016-05-04, retrieved 2016-05-07

[50] "Dr. Craig Wright". Archived from the original on 2016-05-07.

[51] Alex Hern. "Craig Wright U-turns on pledge to provide evidence he invented bitcoin". *the Guardian*.

[52] Nakamoto, Andrew O'Hagan on the many lives of Satoshi (2016-06-30). "The Satoshi Affair". *London Review of Books*. pp. 7–28. ISSN 0260-9592. Retrieved 2016-06-28.

[53] "There could be a lot of money in claiming to have invented Bitoin". Retrieved 2016-06-28.

[54] Davis, Joshua (10 October 2011). "The Crypto-Currency". *The New Yorker*. Retrieved 17 December 2013.

[55] Clear, Michael (4 April 2013). "Clarifications on Bitcoin Article". Retrieved 17 December 2013.

[56] "Who is Satoshi Nakamoto?". coindesk.com. 26 November 2013. Retrieved 17 December 2013.

[57] Penenberg, Adam (11 October 2011). "The Bitcoin Crypto-currency Mystery Reopened". The Fast Company. Retrieved 17 December 2013.

[58] Updating and Distributing Encryption Keys US 20100042841 A1

[59] "I Think I Know Who Satoshi Is". YouTube TheTedNelson Channel. 18 May 2013.

[60] Eileen Ormsby (2013-07-10). "The outlaw cult". Theage.com.au. Retrieved 2013-12-19.

[61] Liu, Alec. "Who Is Satoshi Nakamoto, the Creator of Bitcoin?". vice.com. Retrieved 17 December 2013.

[62] "I am not Satoshi" (blog). Retrieved 2014-02-21.

[63] Markoff, John (23 November 2013). "Study Suggests Link Between Dread Pirate Roberts and Satoshi Nakamoto". New York Times.

[64] Wile, Rob. "Researchers Retract Claim Of Link Between Alleged Silk Road Mastermind And Founder Of Bitcoin". *Business Week*. Retrieved 17 December 2013.

[65] Naughton, John (7 April 2013). "Why Bitcoin scares banks and governments". *The Observer*. Retrieved 11 March 2014.

2.1.5 External links

- *The Satoshi Affair. Andrew O'Hagan on the many lives of Satoshi Nakamoto*

2.2 Hal Finney

Harold Thomas Finney II (May 4, 1956 – August 28, 2014) was a developer for PGP Corporation, and was the second developer hired after Phil Zimmermann. In his early career, he was credited as lead developer on several console games. He also was an early bitcoin user and received the first bitcoin transaction from bitcoin's creator Satoshi Nakamoto.

2.2.1 Early life and education

Finney was born in Coalinga, California, in 1956. He went on to attend the California Institute of Technology, graduating with a BS in engineering in 1981.

2.2.2 Career

After graduation from Caltech, he went to work in the computer gaming field for a company that developed video games such as *Adventures of Tron*, *Armor Ambush*, *Astroblast* and *Space Attack*.[1] He later went to work for the PGP Corporation with whom he remained until his retirement in 2011.[2]

Finney was a noted cryptographic activist.[3] During the early 1990s, in addition to being a regular poster on the cypherpunks listserv, Finney ran two anonymous remailers.[4] Further cryptographic activism included running a (successful) contest to break the export-grade encryption Netscape used.[5]

In 2004, Finney created the first reusable proof of work system before bitcoin.[6] In January 2009, Finney was the bitcoin network's first transaction recipient.[7]

2.2.3 Private life, illness

In October 2009, Finney announced in an essay on the blog Less Wrong that he had been diagnosed with Amyotrophic Lateral Sclerosis (ALS) in August 2009.[8] Prior to his illness, Finney had been an active runner. Finney and his wife Fran Finney raised money for ALS research with the Santa Barbara International Marathon.[9][10][11]

During the last year of his life, the Finneys received anonymous calls demanding an extortion fee of 1,000 bitcoin. They became victims of swatting — a hoax "where the perpetrator calls up emergency dispatch using a spoofed telephone number and pretends to have committed a heinous crime in the hopes of provoking an armed police response to the victim's home".[12]

2.2.4 Death

Hal Finney died in Phoenix August 28, 2014 and was cryopreserved by the Alcor Life Extension Foundation.[2][13][14]

2.2.5 References

[1] "AtariAge". Retrieved 24 February 2015.

[2] Popper, Nathaniel, "Hal Finney, Cryptographer and Bitcoin Pioneer, Dies at 58", *The New York Times*, August 30, 2014

[3] "For instance, many ACLU members do not share the generalized antipathy toward government that is a common premise of "cypherpunk" activists like Hal Finney and Tim May." David Brin, *The Transparent Society* ch2

[4] "Prospects for remailers - Parekh - First Monday". Retrieved 24 February 2015.

[5] "Give Us Some Credit: Your Card is Safe", *The Washington Post*, 1996

[6] "Here's The Problem With The New Theory That A Japanese Math Professor Is The Inventor Of Bitcoin". *SFGate*. Retrieved 24 February 2015.

[7] "Hal Finney received the first Bitcoin transaction. Here's how he describes it.". *Washington Post*. Retrieved 24 February 2015.

[8] "Dying Outside". Retrieved 24 February 2015.

[9] Fight for a Cure for ALS: A Marathoners Story

[10] "Hal and Fran Finney Are Running for a Cause". Retrieved 24 February 2015.

[11] "After a Year of ALS, Reality Begins to Hit Home for Hal and Fran Finney". Retrieved 24 February 2015.

[12] Robert McMillan (29 December 2014). "An Extortionist Has Been Making Life Hell for Bitcoin's Earliest Adopters". *Wired*. Condé Nast. Retrieved 3 January 2015.

[13] Max More (2014-08-28). "Hal Finney being cryopreserved now".

[14] Andy Greenberg (2014-08-28). "Bitcoin's Earliest Adopter Is Cryonically Freezing His Body to See the Future".

2.2.6 External links

- "Hal Finney home page". Archived from the original on 2014-04-03.
- Review: Vernor Vinge's 'Fast Times' (review by Finney in *Extropy*)
- Hal Finney's profile in Forbes Magazine

2.3 Gavin Andresen

Gavin Andresen (born Gavin Bell[1]) is based in Amherst, Massachusetts. After graduating from Princeton University in 1988,[1] Andresen began his career working on 3D graphics software at Silicon Graphics Computer Systems.[2] In 1996, he co-authored the VRML 2.0 specification,[3] and later published a reference manual for VRML 2.0.[4]

Since leaving Silicon Valley in 1996, Andresen has tackled a wide variety of software-related ventures, including CTO of an early voice-over-the-Internet startup and co-founder of a company that made multiplayer online games for blind people and their sighted friends.[2]

In April 2011, Forbes quoted Andresen as saying, "Bitcoin is designed to bring us back to a decentralized currency of the people," and "this is like better gold than gold."[5]

Prior to 2014 Andresen was the lead developer for a part of the bitcoin digital currency project, working to create a secure, stable "cash for the Internet."[6]

Andresen also created ClearCoin, an escrow-type of service, which was closed c. June 23, 2011.[7]

2.3.1 References

[1] Simonite, Tom (15 August 2014). "The Man Who Really Built Bitcoin". *MIT Technology Review*. Massachusetts Institute of Technology. Retrieved 25 August 2014.

[2] "The Future of Payments - Panelists - Bitcoin 2013: The Future of PaymentsMay 17-19, 2013 - San Jose, CA". Bitcoin 2013. 2011-04-16. Retrieved 2014-03-06.

[3] "VRML 2.0".

[4] "The Annotated VRML 2.0 Reference Manual".

[5] "Crypto Currency". Forbes. 2011-04-20. Retrieved 2014-03-06.

[6] "Gavin Andresen Steps Down".

[7] "ClearCoin - Bitcoin". En.bitcoin.it. Retrieved 2014-03-06.

2.3.2 External links

- "Bitcoin Foundation: Transperency: Board Members". Bitcoin Foundation. Retrieved 2015-01-15.
- "Bitcoin 2013: The Future of Payments - Panelists - Bitcoin 2013: The Future of Payments May 17-19, 2013 - San Jose, CA". Bitcoin Foundation. Retrieved 2013-08-07.
- Gavin Andresen interviewed on the TV show Triangulation on the TWiT.tv network 15 May 2013, duration: 60 min.
- *Can Bitcoin Go Mainstream?* Voices of the Next Generation with Gavin Andresen of Bitcoin, Council of Foreign Relations, February 6, 2014

2.4 Nick Szabo

Nick Szabo is a computer scientist, legal scholar and cryptographer known for his research in digital contracts and digital currency. He graduated from the University of Washington in 1989 with a degree in computer science.[1]

The phrase and concept of "smart contracts" was developed by Szabo with the goal of bringing what he calls the “highly evolved” practices of contract law and practice to the design of electronic commerce protocols between strangers on the Internet.[2][3] Smart contracts are a major feature of cryptocurrencies[4][5] and the E programming language.[6]

Szabo influentially[7] argued that a minimum granularity of micropayments is set by mental transaction costs.[8][9]

2.4.1 Bit gold

In 1998, Szabo designed a mechanism for a decentralized digital currency he called “bit gold”.[10][11] Bit gold failed to garner widespread support, but has been called ‘a direct precursor to the Bitcoin architecture.’ [12]

In Szabo’s bit gold scheme, a participant would dedicate computer power to solving cryptographic puzzles. In a bit gold network, solved puzzles would be sent to the Byzantine fault-tolerant public registry and assigned to the public key of the solver. Each solution would become part of the next challenge, creating a growing chain of new property. This aspect of the system provided a way for the network to verify and time-stamp new coins, because unless a majority of the parties agreed to accept new solutions, they couldn’t start on the next puzzle.[13][14]

When attempting to design transactions with a digital coin, you run into the “double-spending problem.” Once data have been created, reproducing them is a simple matter of copying and pasting. Most digital currencies solve the problem by relinquishing some control to a central authority, which keeps track of each account’s balance. This was an unacceptable solution for Szabo. “I was trying to mimic as closely as possible in cyberspace the security and trust characteristics of gold, and chief among those is that it doesn’t depend on a trusted central authority,” he said.[10]

2.4.2 Bitcoin speculation

In 2008, a mysterious figure who wrote under the name Satoshi Nakamoto released a proposal for bitcoin. Nakamoto’s true identity remained a secret, which led to speculation about a long list of people suspected to be Nakamoto. Although Szabo has repeatedly denied it, people have speculated that he is Nakamoto.[15][16]

Research by financial author Dominic Frisby provides circumstantial evidence but, as he admits, no proof that Satoshi is Szabo.[17] Speaking on RT’s *Keiser Report*, he said “I've concluded there is only one person in the whole world that has the sheer breadth but also the specificity of knowledge and it is this chap...”.[18] In a July 2014 email to Frisby, Szabo said: 'Thanks for letting me know. I'm afraid you got it wrong doxing me as Satoshi, but I'm used to it.'[19]

Nathaniel Popper wrote in *The New York Times* that “the most convincing evidence pointed to a reclusive American man of Hungarian descent named Nick Szabo.” In 2008, prior to the release of bitcoin, Szabo wrote a comment on his blog about the intent of creating a live version of his hypothetical currency.[20]

In 2015, the subsequent blockchain Ethereum named a subunit of the Ethereum value token the "Szabo".

2.4.3 References

[1] nytimes.com; “Decoding the enigma of Satoshi Nakamoto and the birth of bitcoin”.

[2] Morris, David Z. “Bitcoin is not just a digital currency. It’s Napster for finance”. Fortune Magazine. Retrieved 6 March 2014.

[3] Szabo, Nick. “Formalizing and Securing Relationships on Public Networks”. First Monday. Retrieved 6 March 2014.

[4] Swanson, Tim. “Smart Property, Colored Coins and Mastercoin”. Coindesk. Retrieved 6 March 2014.

[5] “Counterparty:A distributed financial market”. Retrieved 6 March 2014.

[6] “Smart Contracts in E”. Retrieved 6 March 2014.

[7] Anderson, Chris. *Free: The Future of a Radical Price*. ISBN 1401394515.

[8] Szabo, Nick. “Micropayments and Mental Transaction Costs”. CiteSeerX: 10.1.1.23.9779.

[9] Szabo, Nick. “The Mental Accounting Barrier to Micropayments”. Retrieved 10 December 2013.

[10] Morgan E. Peck (30 May 2012). “Bitcoin, the cryptoanarchists’ answer to cash”. Retrieved 24 June 2015.

[11] Szabo, Nick (December 2005). “Bit gold”. Retrieved 24 June 2015.

[12] Martin O’Leary (8 May 2015). “The Mysterious Disappearance of Satoshi Nakamoto, Founder & Creator of Bitcoin”. Retrieved 24 June 2015.

[13] Tschorsch, Florian; Scheuermann, Björn (15 May 2015). “Bitcoin and Beyond: A Technical Survey of Decentralized Digital Currencies” (PDF). Retrieved 24 June 2015.

[14] Szabo, Nick. “Secure property titles with owner authority”. Retrieved 24 June 2015.

[15] “Who is Satoshi Nakamoto? An Inside Look at the Man Behind Bitcoin”.

[16] “Who Is The Real Satoshi Nakamoto? One Researcher May Have Found The Answer”. *TechCrunch*. 2013-12-05.

[17] Frisby, Dominic (2014) “Who is Satoshi Nakamoto?" In Bitcoin : the Future of Money?, p 85-149. Unbound. ISBN 1783520779

[18] "Nick Szabo is (probably) Satoshi Nakamato". 2014-11-06. Retrieved 2014-11-06. at ~17:30 into the show

[19] Frisby p147

[20] Popper, Nathaniel. "Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin". *New York Times*. Retrieved 15 May 2015.

2.4.4 External links

- Essays and Papers
- Personal Blog
- Nick Szabo on Twitter

2.5 Winklevoss twins

Warning: Page using Template:Infobox sportsperson with unknown parameter "Brother" (this message is shown only in preview).

The **Winklevoss twins** (born August 21, 1981), collectively referred to as the **Winklevi**[1][2] or **Winklevii**,[3] are American rowers and Internet entrepreneurs, Cameron Winklevoss and Tyler Winklevoss. They competed in the men's pair rowing event at the 2008 Beijing Olympics. They are known for co-founding HarvardConnection (later renamed ConnectU) along with Harvard University classmate Divya Narendra. In 2004, the Winklevoss brothers sued Facebook founder Mark Zuckerberg, claiming he stole their ConnectU idea to create the popular social networking site, and ultimately received $65 million.

They are now venture capitalists,[4] and have led a seed funding round for bitcoin payment processor BitInstant.[5] In April 2013, the brothers claimed they owned nearly 1% of all bitcoin in existence at the time.

2.5.1 Early life and education

The Winklevoss twins were born in Southampton, New York, and raised in Greenwich, Connecticut.[6] Their father is Howard Edward Winklevoss, Jr.;[7][8] Howard was a professor of actuarial science at the Wharton School of the University of Pennsylvania.[9] He is the author of *Pension Mathematics with Numerical Illustrations*, and founder of Winklevoss Consultants and Winklevoss Technologies.

The twins went to the Greenwich Country Day School before attending the Brunswick School for high school.[10] They showed a fondness for the classics in high school, studying Latin and Ancient Greek. During their junior year, they co-founded the crew program.[11][12] They enrolled at Harvard University in 2000 for their undergraduate studies where they majored in economics, earning B.A. degrees and graduating in 2004. At Harvard, they were members of the men's varsity crew, the Porcellian Club[13][14] and the Hasty Pudding Club.

In 2009, they began graduate business study at the Saïd Business School at the University of Oxford and completed MBA degrees in 2010.[15] While at Oxford, the brothers were members of Christ Church,[16] and rowed in the Blue Boat in the Oxford-Cambridge Boat Race earning them an Oxford Blue.[17][18]

2.5.2 ConnectU

Main article: ConnectU

ConnectU (originally HarvardConnection) was a social networking website launched on May 21, 2004,[19] that was founded by Harvard students Cameron Winklevoss, Tyler Winklevoss, and Divya Narendra in December 2002.[20] Users could add people as friends, send them messages, and update their personal profiles to notify friends about themselves.[21] Users were placed in networks based upon the domain name associated with the email address they used for registration.[22]

2.5.3 Bitcoin

The twins' company, Math-Based Asset Services LLC, filed to register a bitcoin-based exchange-traded fund called Winklevoss Bitcoin Trust in 2013.[23][24][25]

In 2013, the twins led a $1.5 million in seed funding of BitInstant, a bitcoin payment processor. However, in January 2014, Charlie Shrem, CEO of BitInstant, was arrested and charged with money laundering related to the Silk Road online black market investigation.[26] The brothers said they were passive investors in the company.[25]

In 2014, the twins launched Winkdex, a financial index that tracks the price of bitcoin.[25] The index uses data from seven exchanges, weighed based on the daily trading volume of each exchange.[25]

In March 2014, it was announced that the twins had purchased seats on Richard Branson's Virgin Galactic shuttle using the profits they had made from bitcoin.[27]

In October 2015, Gemini, the twins' Bitcoin exchange, received approval to launch from the New York State Department of Financial Services. The exchange is targeted at both first-time users and professional traders. [28]

2.5.4 Popular culture

Both twins are played by actor Armie Hammer in *The Social Network* (2010), a film directed by David Fincher about the founding of Facebook. Actor Josh Pence was the body double for Tyler with Hammer's face superimposed. In an episode of *The Simpsons*, "The D'oh-cial Network", Patty and Selma take part in the Olympic rowing, and race against the Winklevoss twins, who are voiced by Armie Hammer.[29]

2.5.5 References

[1] Karl M. Aspelund (December 8, 2013). "Winklevi Finally Vindicated?". *Harvard Crimson*. Retrieved February 24, 2015.

[2] James Temple (April 23, 2011). "The Winklevi typify culture of whiners". *San Francisco Chronicle*. Retrieved February 24, 2015.

[3] Killingsworth, Silvia (May 15, 2012). "The Winklevii". *The New Yorker*.

[4] Mashable Video (2012-04-28). "Winklevoss Twins Start Up a Venture Capital Firm [VIDEO]". Mashable.com. Retrieved 2012-12-18.

[5] Taylor, Colleen (May 17, 2013). "With $1.5M Led By Winklevoss Capital, BitInstant Aims To Be The Go-To Site To Buy And Sell Bitcoins". TechCrunch.

[6] "NBC Olympics Cameron Winklevoss Athlete Bio". Retrieved 2010-08-26.

[7] Chamoff, Lisa (March 27, 2010). "Friendships Forged in Devastating Nor-Easter". Greenwich Time.

[8] "Mildred Lotz Leonard Obituary". The Wave. February 9, 2007.

[9] "Winklevoss Technologies About Us". Retrieved 2010-08-21.

[10] Gustafson, Colin (2010-08-16). "Twins back in spotlight with upcoming Facebook film". Greenwich Time.

[11] Riley, Cailin (2008-07-10). "Twin rowers headed to Olympics". The Southampton Press.

[12] Matson, Barbara (2008-07-27). "Rowing Machines: Winklevoss twins hope to form successful pair in Beijing". The Boston Globe.

[13] Ben Mezrich. *The Accidental Billionaires*. p. 28.

[14] "Aaron Sorkin toured Harvard's secret clubs for Facebook film". New York Post. 2010-07-25.

[15] Betts, Hannah (2010-03-20). "Muscle-bound, Oxford-educated and multi-millionaires-meet the Winklevoss twins". London: The Times, The Sunday Times.

[16] Milmo, Cahal (2010-03-03). "Is there anything the Winklevoss twins can't do?". London: The Independent.

[17] Rossingh, Danielle (2010-04-01). "Harvard Twins Who Sue Facebook Now Take on Cambridge in 156th Boat Race". Bloomberg.

[18] Whittle, Natalie (2010-03-05). "Social networking pioneers...and killer oarsmen". Financial Times.

[19] Bombardieri, Marcella (2004-09-17). "Online Adversaries: Rivalry between college-networking websites spawns lawsuit". The Boston Globe.

[20] Pontin, Jason (2007-08-12). "Who owns the concept if no one signs the papers?". The New York Times.

[21] Cassidy, John (2006-05-15). "Me Media: How hanging out on the Internet became big business". The New Yorker.

[22] McGinn, Timothy (2004-05-28). "Online facebooks duel over tangled web of authorship". The Harvard Crimson.

[23] Condon, Christopher (2014-02-02). "Winklevosses' Lawyer in talks with SEC over Bitcoin ETF". *Bloomberg*.

[24] Womack, Brian (2013-07-02). "Winklevoss twins create fund to invest in Bitcoin market". *Bloomberg*.

[25] Popper, Nathaniel (2014-02-19). "Winklevoss brothers offer an index to track price of Bitcoin". *The New York Times*.

[26] Greenberg, Andy (2014-01-27). "Winklevoss-funded Bitcoin startup's CEO arrested in Silk Road investigation". *Forbes*.

[27] Long, Katie (5 March 2014). "The Winklevoss Twins Are Paying to go to Space With Bitcoin". *Slate*. Retrieved 6 March 2014.

[28] Faraz, Tabish. "Winklevoss twins announce launch of Bitcoin exchange Gemini". *www.coinreport.net*. Retrieved 15 October 2015.

[29] Snierson, Dan (2011-07-22). "Armie Hammer to play the Winklevoss twins again... on 'The Simpsons'! -- EXCLUSIVE". *Entertainment Weekly*. Retrieved 2011-07-22.

2.6 Mark Karpelès

Mark Marie Robert Karpelès[1][2] (born June 1, 1985), also sometimes known by his online alias **MagicalTux**, was the CEO of bitcoin exchange Mt. Gox.[3][4] He moved to Japan in 2009.[5][6]

2.6.1 Early life and education

Karpelès was born in 1985 in Chenôve, France, the child of Anne-Robert Karpelès, a geologist.[7] He was raised in Dijon.[7][8] Between 1995 and 2000, Karpelès was educated at Collège Prieuré de Binson in Châtillon-sur-Marne and Prieuré De Binson in Dormans.[3] He then spent one year at Lycée Claude Bernard in Paris, before completing his education in 2003 at Lycée Louis Armand in Paris.[3]

2.6.2 Career

According to Karpelès' LinkedIn page, he worked from 2003 to 2005 at Linux Cyberjoueurs as a software developer and network administrator.[9] Karpelès is a PHP developer, and has contributed to the language's official repository of extensions with proctitle,[10] which allows the name of the current process to be changed on Linux systems.

Karpelès founded Tibanne Co. Ltd. in 2009. He is CEO.[11][12] He was a founding member of the Bitcoin Foundation, created in 2012 with a mission to standardize and promote bitcoin, and served on its board until February 2014.[13][14][15]

Karpelès acquired 88% of the Tokyo-based company Mt. Gox from programmer Jed McCaleb in 2011.[16][17][18] Mt. Gox filed for bankruptcy in Japan on February 28, 2014 and for Chapter 15, Title 11, United States Code bankruptcy in the United States (Texas) in March 2014.[1][19][20]

Karpelès was subpoenaed by the United States Department of the Treasury's Financial Crimes Enforcement Network to appear in Washington, D.C. to provide testimony on April 18, 2014. Karpelès, in a court filing by Mt. Gox lawyers, responded that he does not have a lawyer for this matter and therefore declined to appear.[21][22] Karpelès sought to appear in D.C. to testify on May 5, 2014.[23][24]

According to a joint report by Cyrus Farivar of Ars Technica and Pierre Alonso of Le Monde, Karpelès was found guilty of fraud when he was tried in absentia in France in 2010. He also admitted to having "pirated" a server to French authorities. He was sentenced to a year in jail but has not yet served his sentence.[25][26]

Ross William Ulbricht, while on trial for operating the undercover Silk Road marketplace, claimed in 2015 that the pseudonymous "Dread Pirate Roberts" behind Silk Road was not him but Mark Karpelès.[27] Karpelès publicly denied the claim on Twitter,[28] and Ulbricht was eventually found guilty.[29]

2.6.3 Arrest and prosecution

Karpelès was arrested on 1 August 2015 by Japanese police on suspicion of having accessed the exchange's computer system to falsify data on its outstanding balance,[30][31][32] he was never released but re-arrested and allegedly charged with embezzlement.[33]

2.6.4 References

[1] "Declaration of Mark Marie Mark Karpeles" (PDF). US Bankruptcy Court for the Northern District of Texas Dallas Division: 1. Retrieved 13 March 2014. The document, signed by "Robert Marie Mark Karpeles", was published by *Ars Technica* on the Scribd website, and according to *Ars Technica* is a court document filed in US Bankruptcy Court.

[2] Farivar, Cyrus (2014-03-10). "MtGox files for US bankruptcy protection to put lawsuits on hold". *Ars Technica*.

[3] "Mark Robert KARPELÈS, 28 ans (TOKYO, CHATILLON SUR MARNE, PARIS)". *Copains d'avant – L'Internaute* (in French). CCM Benchmark Group. Retrieved 2014-02-27.

[4] King, Leo (2014-02-26). "Mt. Gox CEO Mark Karpeles: 'I am still in Japan'". *Forbes*. Retrieved 2014-02-27.

[5] Warnock, Eleanor; Mochizuki, Takashi (2014-02-28). "Bitcoin's Mt. Gox: a look at the man in charge". *The Wall Street Journal*.

[6] Philippe, Berry (2014-02-27). "MtGox: Mark Karpèles, un "supergeek" français au cœur du scandale bitcoin". *20 Minutes* (in French). Retrieved 2014-02-27.

[7] Gautronneau, Vincent (2014-01-03). "Le génie côte-d'orien qui fait trembler le net". *Le Journal de Saône et Loire* (in French).

[8] Mick, Jason (March 5, 2014). "Bitcoin King: Mt. Gox CEO Mark Karpelès' History of Arrests, Firings". *DailyTech*. Retrieved March 9, 2014.

[9] Karpeles, Mark. "⍰⍰ Mark Karpelès". LinkedIn. Retrieved 2014-02-27.

[10] "PECL :: Package :: proctitle". Retrieved 24 February 2015.

[11] http://www.cnbc.com/id/101486280

[12] David Meyer. "A Bitcoin Exchange Goes for Respectability". *Businessweek.com*. Retrieved 24 February 2015.

[13] "Mt. Gox resigns from Bitcoin Foundation". *Reuters*. February 23, 2014. Retrieved 25 February 2014.

[14] "Mt. Gox quits Bitcoin Foundation board". *PCWorld*. 24 February 2014. Retrieved 24 February 2015.

[15] Jon Matonis (27 September 2012). "Bitcoin Foundation Launches To Drive Bitcoin's Advancement". *Forbes*. Retrieved 24 February 2015.

[16] Rachel Abrams Matthew Goldstein and Hiroko Tabuchi. "Erosion of Faith Was Death Knell for Mt. Gox". *The New York Times*. Retrieved 24 February 2015.

[17] Jeffries, Adrianne (April 1, 2013). "Barons of Bitcoin". *The Verge*. Retrieved 13 March 2014.

[18] http://online.wsj.com/article/BT-CO-20140310-712183.html

[19] "Bitcoin Exchange Mt. Gox Files for U.S. Bankruptcy as Death Spiral Continues". *WIRED*. Retrieved 24 February 2015.

[20] "Mt. Gox files for Chapter 15 in U.S.". *Market Watch*. Retrieved 13 March 2014.

[21] "Mt. Gox founder won't appear in U.S. for questions about bankruptcy case". *Reuters*. Retrieved 24 February 2015.

[22] "Mt. Gox founder won't attend US bankruptcy hearing". *CNET*. CBS Interactive. Retrieved 24 February 2015.

[23] John Ribeiro (15 April 2014). "Mt. Gox seeks postponement of CEO's U.S. court deposition". *Computerworld*. Retrieved 24 February 2015.

[24] "BBC News - MtGox chief refuses to go to Bitcoin bankruptcy hearing". *BBC News*. Retrieved 24 February 2015.

[25] Farivar, Cyrus (August 1, 2014). "Why the head of Mt. Gox Bitcoin exchange should be in jail". *Ars Technica*. Retrieved August 1, 2014.

[26] Alonso, Pierre (August 1, 2014). "En France, le passé trouble de l'ancien " baron du bitcoin "" [Old bitcoin baron's old trouble in France]. *Le Monde* (in French). Retrieved August 1, 2014.

[27] "UNDERCOVER SILK ROAD AGENT BELIEVED DREAD PIRATE ROBERTS (DPR) TO BE MARK KARPELES OF MT. GOX". Retrieved 16 January 2015.

[28] "Mark Karpeles on Twitter: "This is probably going to be disappointing for you, but I am not and have never been Dread Pirate Roberts."". January 15, 2015. Retrieved January 28, 2015.

[29] Mullin, Joe (4 February 2015). "Ulbricht guilty in Silk Road online drug-trafficking trial". *Ars Technica*. Retrieved 4 February 2015.

[30] "MtGox bitcoin chief Mark Karpeles arrested in Japan". 1 August 2015. Retrieved 1 August 2015.

[31] Jonathan Soble (August 1, 2015). "Mark Karpeles, Chief of Bankrupt Bitcoin Exchange, Is Arrested in Tokyo". *The New York Times*. Retrieved August 1, 2015.

[32] "Mt. Gox bitcoin firm head arrested". *The Japan News by The Yomiuri Shimbun*. August 1, 2015. Retrieved August 1, 2015.

[33] "French MtGox CEO in Japan charged with embezzlement amid bitcoin fraud investigation". *South China Morning Post*. September 11, 2015. Retrieved September 11, 2015.

2.6.5 External links

- Mark Karpelès on Twitter

Chapter 3

Organizations

3.1 Bitcoin Foundation

The **Bitcoin Foundation** is an American nonprofit corporation. It was founded in September 2012 with the stated mission to "standardize, protect and promote the use of bitcoin cryptographic money for the benefit of users worldwide."[1] The organization was modeled on the Linux Foundation and is funded mainly through grants made by for-profit companies that depend on the bitcoin technology.[2]

In March 2014, the Foundation hired Jim Harper of the Cato Institute as Global Policy Counsel and Amy Weiss of Weiss Public Affairs as a media consultant.[3]

3.1.1 History

According to its founding documents, the Bitcoin Foundation's original members included Gavin Andresen, Charlie Shrem, Mark Karpeles, Peter Vessenes, Roger Ver, and Patrick Murck. Current board members are divided into one of three categories: Founding Members, Industry Members, and Individual Members. The board is made up of a combination of elected members of the aforementioned categories.

Former lead bitcoin developer Gavin Andresen is employed by the foundation as "chief scientist."[2] In June 2013, the foundation received media attention when it published a letter from the California Department of Financial Institutions requesting that they "cease and desist from conducting the business of money transmission in this state,"[4] and again when it published their detailed response to the regulators.[5] In November 2013, Patrick Murck, general counsel of the Bitcoin Foundation, testified before a United States Senate committee convened to assess digital currencies, at which the reception of bitcoin by lawmakers was generally positive.[6]

3.1.2 Leadership

Bitcoin Foundation's board of directors, as of May 2014, included chairperson Peter Vessenes, Gavin Andresen, Bobby Lee, Micky Malka, Jon Matonis, Brock Pierce, and Elizabeth Ploshay.[7] In October 2014, Jon Matonis resigned from his position of Executive Director of the Foundation, and at the end of the election cycle on 31 December 2014 stepped down from the group's board of directors.[8]

BTC China CEO Bobby Lee and venture capitalist Brock Pierce were appointed to the foundation's board of directors following a May 2014 runoff election, filling vacancies left by the earlier resignations of former BitInstant CEO Charlie Shrem and Mt. Gox CEO Mark Karpelès.[7] Nine members of the foundation resigned following the May election, citing opposition to the appointments and the direction of the organization.[9]

On 13 April 2015, the board appointed investor and financial consultant Bruce Fenton as Executive Director of the Bitcoin Foundation.[10] At the Blockchain Training Conference / DEVCORE Toronto, the Bitcoin Foundation announced the appointment of Llew Claasen as Executive Director, effective 1 July 2016 [11]

3.1.3 Awards

On 29 March 2016, the Bitcoin Foundation was listed by UK-based company Richtopia at number 27 in the list of 100 Most Influential Blockchain Organisations.[12][13]

3.1.4 Criticism

The Foundation and its leadership have been criticized by some in the media.[14][15] Former vice-chairman Charlie Shrem pleaded guilty to aiding and abetting the operation of an unlicensed money-transmitting business related to his role in assisting agents of the online marketplace Silk Road.[16][17][18] Executive chairman Peter Vessenes' business relationship to former board member Mark Karpeles, the former CEO of collapsed Bitcoin exchange Mt. Gox, has been highlighted as inappropriate.[15] The Foundation has also suffered scrutiny and resignations over its hiring of former child star Brock Pierce.[19]

In November 2014, the Bitcoin Foundation announced that it would seek to wind down its education, outreach and public policy initiatives as it turns its focus to core development. Three surveys conducted earlier by the Bitcoin Foundation suggest that many community members, both inside and outside of the organization, want to see it adopt a stronger focus on bitcoin's open-source technology development.[20] The bitcoin community itself is divided over the role of the Foundation as a community or industry representative.[14] Some libertarian bitcoin advocates have criticized the organization's strategy of political lobbying and participation with federal regulators.[14] In November 2014, Cody Wilson announced his run for board seat in the Bitcoin Foundation, stating "I will run on a platform of the complete dissolution of the Bitcoin Foundation and will begin and end every single one of my public statements with that message." [21]

Professor and author Mark T. Williams criticized the Bitcoin Foundation's priorities, writing in a *Business Insider* editorial that "A Foundation of 'B' players has no business claiming it is a protector of a system that remains vulnerable and untrustworthy."[22]

In early 2015, Jim Harper, a fellow at the Cato Institute and Olivier Janssens, a founder of the Freedom Investment Group, were elected to the Bitcoin Foundation's Board.[23] In July 2015, towards the beginning of his term as board member, Janssens made a public announcement on both the Bitcoin Foundation online forum and Reddit concerning the near-term insolvency of the Bitcoin Foundation, which had been kept secret by the board. As a result of this and a lack of cash flow, various staff were terminated.[24] Following disagreement over the future of the organization—Harper and Janssens having both cast votes to dissolve the Foundation—Harper resigned and Janssens was removed the Board in December 2015.[25]

Although their philosophies and interests differ, Fenton, Janssens and Harper may all be considered reformers.

3.1.5 References

[1] Matonis, Jon (27 September 2012). "Bitcoin Foundation launches to drive bitcoin's advancement". *Forbes*.

[2] Bustillos, Maria (2 April 2013). "The bitcoin boom". *The New Yorker*. Retrieved 30 December 2013.

[3] "Jim Harper joins Bitcoin Foundation as global policy counsel and Amy Weiss as media consultant" (PDF). *Bitcoin Foundation* (Press release). 11 March 2014.

[4] McMillan, Robert (24 June 2013). "California says the Bitcoin Foundation is a money-transferrer". *Wired*. Retrieved 31 December 2013.

[5] Spaven, Emily (3 July 2013). "Bitcoin Foundation issues response to cease and desist warning". *CoinDesk*. Retrieved 31 December 2013.

[6] Lee, Timothy (23 November 2013). "For Bitcoin, a successful charm offensive on the Hill". *Washington Post*. Retrieved 24 November 2013.

[7] Rizzo, Pete (9 May 2014). "Bobby Lee, Brock Pierce join Bitcoin Foundation's board of directors". *CoinDesk*.

[8] Rizzo, Pete (30 October 2014). "Jon Matonis Resigns As Bitcoin Foundation Executive Director". *CoinDesk*.

[9] Hajdarbegovic, Nermin (12 May 2014). "Bitcoin Foundation members resign following appointment controversy". *CoinDesk*.

[10] "The Bitcoin Foundation Welcomes Bruce Fenton as Executive Director". *Bitcoin Foundation*. April 13, 2015. Archived from the original on May 10, 2015. Retrieved March 28, 2016.

[11] "Bitcoin Foundation Appoints Llew Claasen as Executive Director". Retrieved 2016-07-12.

[12] "Top 100 Blockchain Organisations: From CoinDesk to BitPay, These Are the Most Influential Organisations in the Distributed Ledger Space". *Richtopia*. Retrieved 18 June 2016.

[13] "Blockchain Organisations Top 100". *Blockchain Age*. Retrieved 11 May 2016.

[14] Neal, Meghan (May 12, 2014). "Bitcoin is Hiring Lobbyists". *Motherboard.com*. Retrieved May 16, 2014.

[15] Tiku, Nitasha (March 7, 2014). "Whistleblower Threatens to Expose Corruption at Bitcoin Foundation". *ValleyWag*. Retrieved May 16, 2014.

[16] Jerving, Sara (September 6, 2014) "Bitcoin Promoter Charles Shrem Pleads Guilty" *The Wall Street Journal*

[17] Hill, Kashmir (January 27, 2014). "Winklevosses, Bitcoin Community Shocked By Arrest of BitInstant CEO Charlie Shrem". *Forbes.com*. Retrieved May 16, 2014.

[18] Jeffires, Adrianne (January 28, 2014). "Charlie Shrem resigns from the Bitcoin Foundation after arrest". *The Verge*. Retrieved May 16, 2014.

[19] Menn, Joseph (May 16, 2014). "Bitcoin Foundation hit by resignations over new director". *Reuters.com*. Retrieved May 16, 2014.

[20] Higgins, Stan. "Bitcoin Foundation Pledges to Focus Solely on Core Development". *coindesk.com*. Retrieved 19 November 2014.

[21] del Castillo, Michael (22 December 2014). "It's official: Cody Wilson is trying to destroy the Bitcoin Foundation from within". *Upstart*.

[22] Williams, Mark T. (25 February 2014). "Mt Gox: The tower of toxic sludge". *Business Insider*.

[23] "Olivier Janssens and Jim Harper Voted to Bitcoin Foundation Board". *CoinDesk*. Retrieved 2016-03-29.

[24] Pick, Leon (July 4, 2015). "Olivier Janssens: Bitcoin Foundation Has No Money Left". *Financial Magnates*. Retrieved March 28, 2016.

[25] "Two Board Members Exit as Bitcoin Foundation Seeks Funding - CoinDesk". *CoinDesk*. Retrieved 2016-03-29.

3.1.6 External links

- Official website

Chapter 4

Technologies

4.1 Bitcoin network

For a broader coverage related to this topic, see Bitcoin.

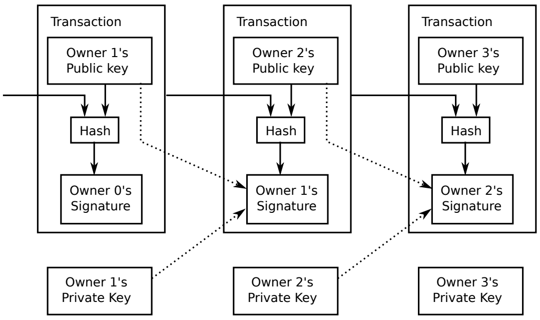
The **bitcoin network** is a peer-to-peer payment network that operates on a cryptographic protocol. Users send bitcoins, the units of currency, by broadcasting digitally signed messages to the network using bitcoin wallet software. Transactions are recorded into a distributed, replicated public database known as the blockchain, with consensus achieved by a proof-of-work system called “mining”. The protocol was designed in 2008 and released in 2009 as open source software by "Satoshi Nakamoto", the name or pseudonym of the original developer/developer group.

The network requires minimal structure to share transactions. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will. Upon reconnection, a node downloads and verifies new blocks from other nodes to complete its local copy of the blockchain.[1][2]

4.1.1 Transactions

A bitcoin is defined by a sequence of digitally signed transactions that began with the bitcoin’s creation as a block reward. The owner of a bitcoin transfers it by digitally signing it over to the next owner using a bitcoin transaction, much like endorsing a traditional bank check. A payee can examine each previous transaction to verify the chain of ownership. Unlike traditional check endorsements, bitcoin transactions are irreversible, which eliminates risk of chargeback fraud.[3]

Although it is possible to handle bitcoins individually, it would be unwieldy to require a separate transaction for every bitcoin in a transaction. Transactions are therefore allowed to contain multiple inputs and outputs,[4] allowing bitcoins to be split and combined. Common transactions will have either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and one or two outputs: one for the payment, and one returning the change, if any, to the sender. Any difference between the total input and output amounts of a transaction goes to miners as a transaction fee.[1]



A diagram of a bitcoin transfer

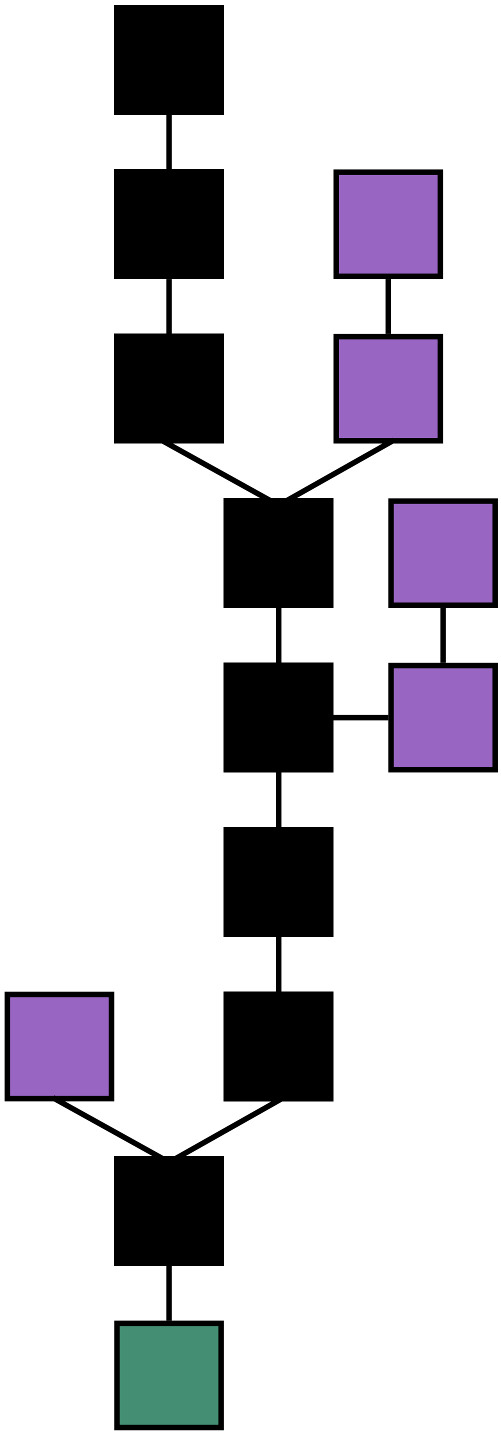
4.1.2 Mining

To form a distributed timestamp server as a peer-to-peer network, bitcoin uses a proof-of-work system similar to Adam Back's Hashcash and the internet rather than newspaper or Usenet posts.[2] The work in this system is what is often referred to as bitcoin mining.

The mining process involves identifying a value that when hashed twice with SHA-256, begins with a number of zero bits. While the average work required increases exponentially with the number of leading zero bits required, a hash can always be verified by executing a single round of double SHA-256.

For the bitcoin timestamp network, a valid “proof-of-work” is found by incrementing a nonce until a value is found that gives the block’s hash the required number of leading zero bits. Once the hashing has produced a valid result, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing the work for each subsequent block.

Majority consensus in bitcoin is represented by the longest chain, which required the greatest amount of effort to produce. If a majority of computing power is controlled by honest nodes, the honest chain will grow fastest and outpace any competing chains. To modify a



The best chain (black) consists of the longest series of transaction records from the genesis block (green) to the current block or record. Orphaned records (purple) exist outside of the best chain.

past block, an attacker would have to redo the proof-of-work of that block and all blocks after it and then surpass the work of the honest nodes. The probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.[2]

To compensate for increasing hardware speed and varying interest in running nodes over time, the difficulty of finding a valid hash is adjusted roughly every two weeks. If blocks are generated too quickly, the difficulty increases and more hashes are required to make a block and to generate new bitcoins.[2]

Bitcoin mining is a competitive endeavor. An "arms race" has been observed through the various hashing technologies that have been used to mine bitcoins: basic CPUs, high-end GPUs common in many gaming computers, FPGAs and ASICs all have been used, each reducing the profitability of the less-specialized technology. Bitcoin-specific ASICs are now available.[5] As bitcoins become more difficult to mine, computer hardware manufacturing companies have seen an increase in sales of high-end products.[6]

Computing power is often bundled together or “pooled” to reduce variance in miner income. Individual mining rigs often have to wait for long periods to confirm a block of transactions and receive payment. In a pool, all participating miners get paid every time a participating server solves a block. This payment is proportional to the amount of work an individual miner contributed to help find that block.[7]

Process

A rough overview of the process to mine bitcoins is:[2]

1. New transactions are broadcast to all nodes.
2. Each miner node collects new transactions into a block.
3. Each miner node works on finding a proof-of-work code for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Receiving nodes validate the transactions it holds and accept only if all are valid.
6. Nodes express their acceptance by moving to work on the next block, incorporating the hash of the accepted block.

Mined bitcoins

By convention, the first transaction in a block is a special transaction that produces new bitcoins owned by the creator of the block. This is the incentive for nodes to support the network.[1] It provides the way to move new bitcoins into circulation.

4.1.3 Local system resources

Once the latest transaction of a coin is buried under enough blocks, fully spent transactions that preceded it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle tree, with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes need not be stored.[1]

4.1.4 Payment verification

Upon receiving a new transaction a node must validate it: in particular, verify that none of the transaction's inputs have been previously spent. To carry out that check the node needs to access the blockchain. Any user who does not trust his network neighbors, should keep a full local copy of the blockchain, so that any input can be verified.

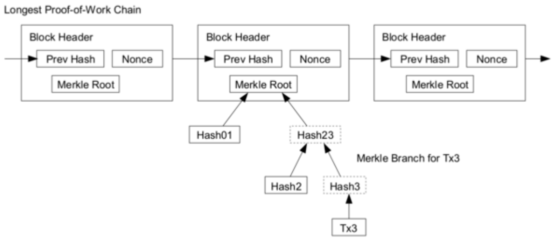


Diagram showing how Bitcoin transactions can be verified

As noted in Nakamoto's whitepaper, it is possible to verify bitcoin payments without running a full network node (simplified payment verification, SPV). A user only needs a copy of the block headers of the longest chain, which are available by querying network nodes until it is apparent that the longest chain has been obtained. Then, get the Merkle branch linking the transaction to its block. Linking the transaction to a place in the chain demonstrates that a network node has accepted it, and blocks added after it further establish the confirmation.[1]

4.1.5 See also

- Blockchain (database) § Sidechains

4.1.6 References

[1] Nakamoto, Satoshi (24 May 2009). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). Retrieved 20 December 2012.

[2] Barber, Simon; Boyen, Xavier; Shi, Elaine & Uzun, Ersin (2012). "Bitter to Better — how to make Bitcoin a better currency" (PDF). *Financial Cryptography and Data Security*. Springer Publishing.

[3] Dean, Andrew (14 August 2014). "Online Gambling Meets Bitcoin". Retrieved 21 August 2014.

[4] "Block Chain Overview". *bitcoin.org/*. © Bitcoin Project 2009-2014 Released under the MIT license. 2009–2014. Retrieved 14 August 2014.

[5] Tindell, Ken (5 April 2013). "Geeks Love The Bitcoin Phenomenon Like They Loved The Internet In 1995". Business Insider.

[6] "Bitcoin boom benefiting TSMC: report". Taipei Times. 4 January 2014.

[7] Biggs, John (8 April 2013). "How To Mine Bitcoins". Techcrunch.

4.2 Cryptocurrency

A **cryptocurrency** (or **crypto currency**) is a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency.[1] Cryptocurrencies are a subset of alternative currencies, or specifically of digital currencies.

Bitcoin became the first decentralized cryptocurrency in 2009.[2] Since then, numerous cryptocurrencies have been created.[3] These are frequently called *altcoins*, as a blend of *bitcoin alternative*.[4][5]

Cryptocurrencies use decentralized control[6] as opposed to centralized electronic money/centralized banking systems.[7] The decentralized control is related to the use of bitcoin's blockchain transaction database in the role of a distributed ledger.[8]

4.2.1 Overview

Decentralized cryptocurrency is produced by the entire cryptocurrency system collectively, at a rate which is defined when the system is created and which is publicly known. In centralized banking and economic systems such as the Federal Reserve System, corporate boards or governments control the supply of currency by printing units of fiat money or demanding additions to digital banking ledgers. However, companies or governments cannot produce units of cryptocurrency and as such, have not so far provided backing for other firms, banks or corporate entities which hold asset value measured in a decentralized cryptocurrency. The underlying technical system upon which decentralized cryptocurrencies are based was created by the group or individual known as Satoshi Nakamoto.[9][10][11]

As of March 2015, hundreds of cryptocurrency specifications exist; most are similar to and derived from the first fully implemented decentralized cryptocurrency, bitcoin.[12][13] Within cryptocurrency systems the safety, integrity and balance of ledgers is maintained by a community of mutually distrustful parties referred to as miners: members of the general public using their computers to help validate and timestamp transactions adding them to the ledger in accordance with a particular timestamping scheme.[14]

The security of cryptocurrency ledgers is based on the assumption that the majority of miners are honestly trying to maintain the ledger, having financial incentive to do so.

Most cryptocurrencies are designed to gradually decrease production of currency, placing an ultimate cap on the total amount of currency that will ever be in circulation, mimicking precious metals.[1][15] Compared with ordinary currencies held by financial institutions or kept as cash on hand, cryptocurrencies are less susceptible to seizure by law enforcement.[1][16] Existing cryptocurrencies are all pseudo-anonymous, though additions such as Zerocoin and its distributed laundry[17] feature have been suggested, which would allow for true anonymity.[18][19][20]

4.2.2 History

In 1998, Wei Dai published a description of "b-money", an anonymous, distributed electronic cash system.[21] Shortly thereafter, Nick Szabo created "Bit Gold".[22] Like bitcoin and other cryptocurrencies that would follow it, Bit Gold was an electronic currency system which required users to complete a proof of work function with solutions being cryptographically put together and published. A currency system based on a reusable proof of work was later created Hal Finney who followed the work of Dai and Szabo.

The first decentralized cryptocurrency, bitcoin, was created in 2009 by pseudonymous developer Satoshi Nakamoto. It used SHA-256, a cryptographic hash function, as its proof-of-work scheme.[23][24][25] In April 2011, Namecoin was created as an attempt at forming a decentralized DNS, which would make internet censorship very difficult. Soon after, in October 2011, Litecoin was released. It was the first successful cryptocurrency to use scrypt as its hash function instead of SHA-256. Another notable cryptocurrency, Peercoin was the first to use a proof-of-work/proof-of-stake hybrid.[26] Many other cryptocurrencies have been created though few have been successful, as they have brought little in the way of technical innovation.[27] On 6 August 2014, the UK announced its Treasury had been commissioned to do a study of cryptocurrencies, and what role, if any, they can play in the UK economy. The study was also to report on whether regulation should be considered.[28]

Publicity

Central bank representatives have stated that the adoption of cryptocurrencies such as bitcoin pose a significant challenge to central banks' ability to influence the price of credit for the whole economy.[29] They have also stated that as trade using cryptocurrencies become more popular, there is bound to be a loss of consumer confidence in fiat currencies.[30] Gareth Murphy, a senior central banking officer has stated "widespread use [of cryptocurrency] would also make it more difficult for statistical agencies to gather data on economic activity, which are used by governments to steer the economy". He cautioned that virtual currencies pose a new challenge to central banks' control over the important functions of monetary and exchange rate policy.[31]

Jordan Kelley, founder of Robocoin, launched the first bitcoin ATM in the United States on February 20, 2014. The kiosk installed in Austin, Texas is similar to bank ATMs but has scanners to read government-issued identification such as a driver's license or a passport to confirm users' identities.[32]

The Dogecoin Foundation, a charitable organization centered around Dogecoin and co-founded by Dogecoin co-creator Jackson Palmer, donated more than $30,000 worth of Dogecoin to help fund the Jamaican bobsled team's trip to the 2014 Olympic games in Sochi, Russia.[33] The growing community around Dogecoin is looking to cement its charitable credentials by raising funds to sponsor service dogs for children with special needs.[34]

4.2.3 Legality

The legal status of cryptocurrencies varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed their use and trade, others have banned or restricted it. Likewise, various government agencies, departments, and courts have classified bitcoins differently. China Central Bank banned the handling of bitcoins by financial institutions in China during an extremely fast adoption period in early 2014.[35] In Russia, though cryptocurrencies are legal, it is illegal to actually purchase goods with any currency other than the Russian ruble.[36]

On March 25, 2014, the United States Internal Revenue Service (IRS) ruled that bitcoin will be treated as property for tax purposes as opposed to currency. This means bitcoin will be subject to capital gains tax. One benefit of this ruling is that it clarifies the legality of bitcoin. No longer do investors need to worry that investments in or profit made from bitcoins are illegal or how to report them to the IRS.[37] In a paper published by researchers from Oxford and Warwick it was shown that bitcoin has some characteristics similar to the precious metals market more than to traditional currencies, hence in agreement to the IRS decision even if based on different reasons.[38]

Legal issues not dealing with governments have also arisen for cryptocurrencies. Coinye, for example, is an altcoin that used rapper Kanye West as its logo without permission. Upon hearing of the release of Coinye, originally called Coinye West, attorneys for Kanye West sent a cease and desist letter to the email operator of Coinye, David P. McEnery Jr. The letter stated that Coinye was willful trademark infringement, unfair competition, cyberpiracy, and dilution and instructed Coinye to stop using the likeness and name of Kanye West.[39]

Concerns of an unregulated global economy

As the popularity of and demand for online currencies increases since the inception of bitcoin in 2009,[40] so do concerns that such an unregulated person to person global economy that cryptocurrencies offer may become a threat to society. Concerns abound that altcoins may become tools for anonymous web criminals.[41]

Cryptocurrency networks display a marked lack of regulation that attracts many users who seek decentralized exchange and use of currency, however these very same lack of regulations have been critiqued as potentially enabling criminals who seek to evade taxes and launder money.

Transactions that occur through the use and exchange of these altcoins are independent from formal banking systems, and therefore can make tax evasion simpler for individuals. Since charting taxable income is based upon what a recipient reports to the revenue service, it becomes extremely difficult to account for transactions made using existing cryptocurrencies, a mode of exchange that is complex (and in some cases impossible) to track.[41]

Systems of anonymity that most cryptocurrencies offer can also serve as a simpler means to launder money. Rather than laundering money through an intricate net of financial actors and offshore bank accounts, laundering money through altcoins stands outside institutions and can be achieved through anonymous transactions.[41] Laundering services for cryptocurrency exist to service the bitcoin currency, in which multiple sourced bitcoins are blended to obscure the relationship between input and output addresses.[41]

Arrests

There have been arrests in the United States related to cryptocurrency. A notable case was the arrest of Charlie Shrem, the CEO of BitInstant.[42][43]

Fraud

On August 6, 2013, Magistrate Judge Amos Mazzant of the Eastern District of Texas federal court ruled that because cryptocurrency (expressly bitcoin) can be used as money (it can be used to purchase goods and services, pay for individual living expenses, and exchanged for conventional currencies), it is a currency or form of money. This ruling allowed for the SEC to have jurisdiction over cases of securities fraud involving cryptocurrency.[44]

GBL, a Chinese bitcoin trading platform, suddenly shut down on October 26, 2013. Subscribers, unable to log in, lost up to $5 million worth of bitcoin.[45][46][47]

In February 2014, cryptocurrency made national headlines due to the world's largest bitcoin exchange, Mt. Gox, declaring bankruptcy. The company stated that it had lost nearly $473 million of their customer's bitcoins likely due to theft. This was equivalent to approximately 750,000 bitcoins, or about 7% of all the bitcoins in existence. Due to this crisis, among other news, the price of a bitcoin fell from a high of about $1,160 in December to under $400 in February.[48]

On March 31, 2015, two now-former agents from the Drug Enforcement Administration and the U.S. Secret Service were charged with wire fraud, money laundering and other offenses for allegedly stealing bitcoin during the federal investigation of Silk Road, an underground illicit black market federal prosecutors shut down in 2013.[49]

On December 1, 2015, the owner of the now-defunct GAW Miners website was accused of securities fraud following his development of the cryptocurrency known as Paycoin. He is accused of masterminding an elaborate ponzi scheme under the guise of "cloud mining" with mining equipment hosted in a data center. He purported the cloud miners known as "hashlets" to be mining cryptocurrency within the Zenportal "cloud" when in fact there were no miners actively mining cryptocurrency. Zenportal had over 10,000 users that had purchased hashlets for a total of over 19 million U.S. dollars.[50][51]

On August 24, 2016, a federal judge in Florida certified a class action lawsuit[52] against defunct cryptocurrency exchange Cryptsy and Cryptsy's owner. He is accused of misappropriating millions of dollars of user deposits, destroying evidence, and is believed to have fled to China.[53]

Darknet markets

Main article: Darknet market

Cryptocurrency is also used in controversial settings in the form of online black markets, such as Silk Road. The original Silk Road was shut down in October 2013 and there have been two more versions in use since then; the current version being Silk Road 3.0. The successful format of Silk Road has been widely used in online dark markets, which has led to a subsequent decentralization of the online dark market. In the year following the initial shutdown of Silk Road, the number of prominent dark markets increased from four to twelve, while the amount of drug listings increased from 18,000 to 32,000.[41]

Darknet markets present growing challenges in regard to legality. Bitcoins and other forms of cryptocurrency used in dark markets are not clearly or legally classified in almost all parts of the world. In the U.S., bitcoins are labelled as "virtual assets". This type of ambiguous classification puts mounting pressure on law enforcement agencies around the world to adapt to the shifting drug trade of dark markets.[54]

Since most darknet markets run through Tor, they can be found with relative ease on public domains. This means that their addresses can be found, as well as customer reviews and open forums pertaining to the drugs being sold on the market, all without incriminating any form of user.[41] This kind of anonymity enables users on both sides of dark markets to escape the reaches of law enforcement. The result is that law enforcement adheres to a campaign of singling out individual markets and drug dealers to cut down supply. However, dealers and suppliers are able to stay one step ahead of law enforcement, who cannot keep up with the rapidly expanding and anonymous marketplaces of dark markets.[54]

4.2.4 Timestamping

Cryptocurrencies use various timestamping schemes to avoid the need for a trusted third party to timestamp transactions added to the blockchain ledger.

Proof-of-work schemes

The first timestamping scheme invented was the proof-of-work scheme. The most widely used proof-of-work schemes are based on SHA-256, which was introduced by bitcoin, and scrypt, which is used by currencies such as Litecoin.[26] The latter now dominates over the world of cryptocurrencies, with at least 480 confirmed implementations.[55]

Some other hashing algorithms that are used for proof-of-work include CryptoNight, Blake, SHA-3, and X11.

Proof-of-stake and combined schemes

Some cryptocurrencies use a combined proof-of-work/proof-of-stake scheme.[26][56] The proof-of-stake is a method of securing a cryptocurrency network and achieving distributed consensus through requesting users to show ownership of a certain amount of currency. It is different from proof-of-work systems that run difficult hashing algorithms to validate electronic transactions. The scheme is largely dependent on the coin, and there's currently no standard form of it.

4.2.5 Economics

Cryptocurrencies are used primarily outside existing banking and governmental institutions, and exchanged over the Internet. While these alternative, decentralized modes of exchange are in the early stages of development, they have the unique potential to challenge existing systems of currency and payments.

Competition in cryptocurrency markets

Today, there are over 700[57] digital currencies in existence. Entry into the marketplace is undertaken by so many due to the low cost of entry and opportunity for profit making through the creation of coins.

Network effects play an important role in analyzing the development of cryptocurrency markets. Since any given currency gains use value as the number of its users increase, popularity of a certain currency is integral in that currency's success. Economists postulate that large competitors (such as the most popular cryptocurrency: bitcoin) will attract more new users due to the size of their growing exchange pools and as a result will effectively dominate the market.

A study entitled “Competition in the Cryptocurrency Market” conducted by members of the NET Institute over three periods between 2013 and 2014 charts the analysis of changes in price data over time in regards to budding cryptocurrency markets. It analyzes bitcoin and other similar cryptocurrencies referred to as “altcoins”. These include Litecoin, Peercoin, and Namecoin; cryptocurrencies listed in order by which account for the largest percentages of digital market capitalization behind bitcoin (which accounts for 90%).

The NET study found that of these four, all were early entrants into the digital currency marketplace, designed to correct perceived bitcoin's flaws and amass popularity in an infant market whose popularity was rapidly growing. This study introduced the question of the role of demand in cryptocurrency markets, and what impetus demand has in relation to emerging coins. The study dealt namely with two common forces of demand that shaped the market: reinforcement and substitution effects. The reinforcement effect expects demand to increase based on usership, and that the cryptocurrency that could gain the most buyers and sellers would win out above all others, thus dominating the marketplace. The substitution effect implies that as the price of bitcoins rose with increased usership, people would begin to look for other options in the cryptocurrency market, thus discouraging any one coin from gaining complete dominance.

Indices

In order to follow the development of the market of cryptocurrencies, indices keep track of notable cryptocurrencies and their cumulative market value.

Crypto Index - CRIX The cryptocurrency index CRIX is a conceptual measurement jointly developed by statisticians at Humboldt University of Berlin, Singapore Management University and the enterprise CoinGecko and was launched in 2016.[58] The index represents cryptocurrency market characteristics dating back until July 31, 2014.[59] Its algorithm takes into account that the cryptocurrency market is frequently changing, with the continuous creation of new cryptocurrencies and infrequent trading of some of the existing ones.[60][61] Therefore, the number of index members is adjusted quarterly according to their relevance on the cryptocurrency market as a whole.[59] It is the first dynamic index reflecting changes on the cryptocurrency market.

4.2.6 List

Main article: List of cryptocurrencies

4.2.7 Academic studies

Journals

In September 2015, the establishment of the peer-reviewed academic journal *Ledger* (ISSN 2379-5980) was announced. It will cover studies of cryptocurrencies and related technologies, and is published by the University of Pittsburgh.[62][63] The journal encourages authors to digitally sign a file hash of submitted papers, which will then be timestamped into the bitcoin blockchain. Authors are also asked to include a personal bitcoin address in the first page of their papers.[64][65]

4.2.8 Criticism

- In 2013, journalists Joshua Brustein and Timothy Lee expressed concern that bitcoin is problematic due to its high volatility.[66]
- In December 2013, Jason O'Grady reported on various pump and dump schemes in altcoins distinct from bitcoin and Litecoin.[67]
- Community refers to premining, hidden launches, or extreme rewards for the altcoin founders as a deceptive practice,[68] but it can also be used as an inherent part of a digital cryptocurrency's design, as in the case of Ripple.[69] Pre-mining means currency is generated by the currency's founders prior to mining code being released to the public.[70]
- Most cryptocurrencies are duplicates of existing cryptocurrencies with minor changes and no novel technical developments. One such, Coinye West, a comedy cryptocurrency alluding to the rapper Kanye West, was served a cease-and-desist letter on 7 January 2014, for using West's name and implying a connection that did not exist.[71]
- Banks generally do not offer services for cryptocurrencies and sometimes refuse to offer services to virtual-currency companies.[72]
- There are ways to permanently lose cryptocurrency from local storage due to malware or data loss. This can also happen through the destruction of the physical media, effectively removing lost cryptocurrencies forever from their markets.[73]
- There are many perceived criteria that cryptocurrencies must reach before they can become mainstream. For example, the number of merchants accepting cryptocurrencies is increasing, but still only a few merchants accept them.[74]
- With technological advancement in cryptocurrencies such as bitcoin, the cost of entry for miners requiring specialized hardware and software is high.[75]
- Cryptocurrency transactions are normally irreversible after a number of blocks confirm the transaction. One of the features cryptocurrency lacks in comparison to credit cards is consumer protection against fraud, such as chargebacks.[14]
- Some coins may be a project with little to no community backing and no visible developer.[76]
- While cryptocurrencies are digital currencies that are managed through advanced encryption techniques, many governments have taken a cautious approach toward them, fearing their lack of central control and the effects they could have on financial security.[77]
- Environmentally conscious people are concerned with the enormous amount of energy that goes into cryptocurrency mining with little to show in return, but it is important to compare it to the consumption of the legacy financial system.[78]
- Traditional financial products have strong consumer protections. However, if bitcoins are lost or stolen, there is no intermediary with the power to limit consumer losses.[79]
- Regulators in several countries have warned against their use and some have taken concrete regulatory measures to dissuade users.[80]
- The success of some cryptocurrencies has caused multi-level marketing schemes to arise with pseudo cryptocurrencies, such as Onecoin.

4.2.9 See also

- Blockchain (database)
- Cryptocurrency tumbler
- Cryptographic protocol
- Digital currency exchanger
- Virtual currency

4.2.10 References

[1] Andy Greenberg (20 April 2011). "Crypto Currency". Forbes.com. Retrieved 8 August 2014.

[2] Sagona-Stophel, Katherine. "Bitcoin 101 white paper" (PDF). Thomson Reuters. Retrieved 11 July 2016.

[3] Tasca, Paolo (7 September 2015). "Digital Currencies: Principles, Trends, Opportunities, and Risks". Social Science Research Network. Retrieved 21 January 2016.

[4] "Altcoin". Investopedia. Retrieved 8 January 2015.

[5] Wilmoth, Josiah. "What is an Altcoin?". cryptocoinsnews.com. Retrieved 4 March 2015.

[6] McDonnell, Patrick "PK" (9 September 2015). "What Is The Difference Between Bitcoin, Forex, and Gold". NewsBTC. Retrieved 15 September 2015.

[7] Allison, Ian (8 September 2015). "If Banks Want Benefits Of Blockchains, They Must Go Permissionless". NewsBTC. Retrieved 15 September 2015.

[8] "All you need to know about Bitcoin". *timesofindia-economictimes*.

[9] Bitcoin-block-signing History, http://blockchain.info, 2 March 2014

[10] Deflation and Banking, http://www.econlib.org, 19 December 2006

[11] Bitcoin Creation Mechanism, https://en.bitcoin.it, 12 January 2014

[12] Listing of active coins, http://cryptocoincharts.info, 27 February 2014

[13] another authentication protocol forked from P.O.S., https://en.bitcoin.it, 7 June 2013

[14] Jerry Brito and Andrea Castillo (2013). "Bitcoin: A Primer for Policymakers" (PDF). *Mercatus Center*. George Mason University. Retrieved 22 October 2013.

[15] How Cryptocurrencies Could Upend Banks' Monetary Role, American Banker, 26 May 2013

[16] The FBI's Plan For The Millions Worth Of Bitcoins Seized From Silk Road, Forbes, 4 October 2013

[17] "Zerocoin - Making bitcoin anonymous". *cryptographyengineering.com*. 2013. Retrieved 2 June 2014.

[18] 'Zerocoin' Add-on For Bitcoin Could Make It Truly Anonymous And Untraceable, Forbes, 26 May 2013

[19] Matthew Green (26 May 2013). "Zerocoin: Anonymous Distributed E-Cash from Bitcoin" (pdf). Johns Hopkins University.

[20] This is Huge: Gold 2.0 - Can code and competition build a better Bitcoin?, New Bitcoin World, 26 May 2013

[21] Wei Dai (1998). "B-Money".

[22] "Bitcoin: The Cryptoanarchists' Answer to Cash". IEEE Spectrum. Around the same time, Nick Szabo, a computer scientist who now blogs about law and the history of money, was one of the first to imagine a new digital currency from the ground up. Although many consider his scheme, which he calls "bit gold," to be a precursor to Bitcoin

[23] Brito, Jerry; Castillo, Andrea (31 August 2013). "Bitcoin: A primer for policy makers" (PDF). *Mercatus Center*. George Mason University. Retrieved 31 October 2015.

[24] What is Bitcoin Mining?, The Genesis Block, 26 May 2013

[25] Bitcoin developer chats about regulation, open source, and the elusive Satoshi Nakamoto, PCWorld, 26-05-2013

[26] Wary of Bitcoin? A guide to some other cryptocurrencies, ars technica, 26-05-2013

[27] "Are Any Altcoins Currently Useful? No, Says Monero Developer Riccardo Spagni". *Bitcoin Magazines*. Retrieved 31 May 2016.

[28] "UK launches initiative to explore potential of virtual currencies". *The UK News*. Retrieved 8 August 2014.

[29] "Central Banks Face 3 New Dilemmas in the Era of Bitcoin and Digital Currencies". *Bitcoin Magazine*. Retrieved 31 May 2016.

[30] "How Bitcoin Compares to Fiat Currency's House of Cards". *Bitcoin Magazine*. Retrieved 31 May 2016.

[31] decentralized currencies impact on central banks, rte News, 3 April 2014

[32] First U.S. Bitcoin ATMs to open soon in Seattle, Austin, Reuters, 18 February 2014

[33] Dogecoin Users Raise $30,000 to Send Jamaican Bobsled Team to Winter Olympics, Digital Trends, 20 January 2014

[34] Dogecoin Community Raising $30,000 for Children's Charity, International Business Times, 4 February 2014

[35] "The Big Picture Behind the News of China's Bitcoin Bans – Bitcoin Magazine". *Bitcoin Magazine*. Retrieved 24 February 2015.

[36] Bitcoin's Legality Around The World, Forbes, 31 January 2014

[37] 3 Reasons The IRS Bitcoin Ruling Is Good For Bitcoin, Nasdaq, 24 March 2014

[38] On the Complexity and Behaviour of Cryptocurrencies Compared to Other Markets, 7 November 2014

[39] Infringement of Kayne West Mark and Other Violations, Pryor Cashman LLP, 6 January 2014

[40] Iwamura, Mitsuru and Kitamura, Yukinobu and Matsumoto, Tsutomu, Is Bitcoin the Only Cryptocurrency in the Town? Economics of Cryptocurrency And Friedrich A. Hayek (February 28, 2014). Available at SSRN: http://ssrn.com/abstract=2405790 or doi:10.2139/ssrn.2405790

[41] ALI, S, T; CLARKE, D; MCCORRY, P; Bitcoin: Perils of an Unregulated Global P2P Currency [By S. T Ali, D. Clarke, P. McCorry Newcastle upon Tyne: Newcastle University: Computing Science, 2015. (Newcastle University, Computing Science, Technical Report Series, No. CS-TR-1470)

[42] http://blogs.wsj.com/law/2015/03/30/bitcoin-entrepreneur-charlie-shrem-reports-to-prison/

[43] "Tracking the Intangible: How Fraud Examiners Are Busting Bitcoin Fraud". Retrieved 24 February 2015.

[44] SEC v Shavers, United States District Court Eastern District Of Texas, 08-06-2013

[45] Vanishing Bitcoins: $5 million in crypto-currency lost down a Chinese memory hole, 21st Century Wire, 12-11-2013

[46] "Banshee bitcoins: $5 million worth of bitcoin vanish in China". Russia Today. Retrieved 6 March 2015.

[47] "When bitcoins go bad: 4 stories of fraud, hacking, and digital currencies.". Washington Post. Retrieved 6 March 2015.

[48] Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss, Carter Dougherty and Grace Huang, Bloomberg News, Feb. 28, 2014

[49] Perez, Evan. "CNN Justice Reporter". CNN. Retrieved 31 March 2015.

[50] Farivar, Cyrus. "Pissed-off customers sue GAW Miners in proposed class-action suit". *Ars Technica*. Retrieved 6 June 2016.

[51] https://www.sec.gov/litigation/complaints/2015/comp23415.pdf

[52] https://www.pacermonitor.com/public/case/10497012/Liu_v_Project_Investors,_Inc_et_al

[53] http://cryptsyreceivership.com/v1/wp-content/uploads/2016/08/Notice-of-Filing-Receivers-2nd-Report-8-2-16-full.pdf

[54] Raeesi, Reza (2015-04-23). "The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can this Storm Be Weathered?". *Glendon Journal of International Studies / Revue d'études internationales de Glendon*. **8** (1-2). ISSN 2291-3920.

[55] "CryptoCoinTalk.com - Discussing the World of Cryptocurrencies". *CryptoCoinTalk*. Retrieved 24 February 2015.

[56] Sunny King, Scott Nadal (19 August 2012). "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake" (PDF). Retrieved 12 May 2013.

[57] "coinmarketcap.com". Retrieved 13 July 2016.

[58] "CRIX - CRypto IndeX". *crix.hu-berlin.de*. Retrieved 2016-08-12.

[59] "CRIX or evaluating blockchain based currencies" ,ISSN 1860-5664, SFB 649 Discussion Paper 2016-021, Simon Trimborn, Wolfgang Karl Härdle, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800928http://crix.hu-berlin.de/data/CRIXDiscussionPaper.pdf, June 15, 2016

[60] "What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis", Ladislav Kristoufek, page 1, Section 1 Introduction, "(the) success has ignited an exposition of new alternative crypto-currencies" https://arxiv.org/abs/1406.0268, Mon, 2 Jun 2014

[61] "Crypto-Currency Market Capitalizations".

[62] "Introducing Ledger, the First Bitcoin-Only Academic Journal". *Motherboard*.

[63] "Bitcoin Peer-Reviewed Academic Journal 'Ledger' Launches". *CoinDesk*.

[64] "Editorial Policies". *ledgerjournal.org*.

[65] "How to Write and Format an Article for Ledger" (PDF). *Ledger*. 2015. doi:10.5195/LEDGER.2015.1.

[66] "Bitcoin's Volatility Problem: Why Today's Selloff Won't Be the Last". Businessweek. 5 December 2013. Retrieved 29 December 2013.

[67] "A crypto-currency primer: Bitcoin vs. Litecoin". ZDNet. 14 December 2013. Retrieved 29 December 2013.

[68] "Scamcoins". August 2013.

[69] Bradbury, Danny (25 June 2013). "Bitcoin's successors: from Litecoin to Freicoin and onwards". *The Guardian*. Guardian News and Media Limited. Retrieved 11 January 2014.

[70] Morris, David Z (24 December 2013). "Beyond bitcoin: Inside the cryptocurrency ecosystem". *CNNMoney, a service of CNN, Fortune & Money*. Cable News Network. Retrieved 11 January 2014.

[71] "Kanye West's lawyer orders "Coinye" to cease and desist just before launch". *Ars Technica*. Retrieved 24 February 2015.

[72] Sidel, Robin (22 December 2013). "Banks Mostly Avoid Providing Bitcoin Services. Lenders Don't Share Investors' Enthusiasm for the Virtual-Currency Craze". Online.wsj.com. Retrieved 29 December 2013.

[73] Keeping Your Cryptocurrency Safe, Center for a Stateless Society, 1 April 2014

[74] The Future of Cryptocurrency, Investopedia, 10 September 2013

[75] Want to make money off Bitcoin mining? Hint: Don't mine, *The Week,* 15 April 2013

[76] Fundamental Analysis for Cryptocurrency, Wall Street Crypto, 10 January 2014

[77] Cryptocurrency and Global Financial Security Panel at Georgetown Diplomacy Conf, MeetUp, 11 April 2014

[78] Experiments in Cryptocurrency Sustainability, Let's Talk Bitcoin, March 2014

[79] Four Reasons You Shouldn't Buy Bitcoins, Forbes, 3 April 2013

[80] Schwartzkopff, Frances (17 December 2013). "Bitcoins Spark Regulatory Crackdown as Denmark Drafts Rules". Bloomberg. Retrieved 29 December 2013.

4.2.11 Further reading

- Chayka, Kyle (2 July 2013). "What Comes After Bitcoin?". Pacific Standard. Retrieved 18 January 2014.
- Guadamuz, Andres; Marsden, Chris (2015). "Blockchains and Bitcoin: Regulatory responses to cryptocurrencies". *First Monday*. **20** (12). doi:10.5210/fm.v20i12.6198.

4.2.12 External links

- Media related to Cryptocurrency at Wikimedia Commons

4.3 Elliptic Curve Digital Signature Algorithm

In cryptography, the **Elliptic Curve Digital Signature Algorithm** (**ECDSA**) offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography.

4.3.1 Key and signature-size comparison to DSA

As with elliptic-curve cryptography in general, the bit size of the public key believed to be needed for ECDSA is about twice the size of the security level, in bits. For example, at a security level of 80 bits (meaning an attacker requires the equivalent of about 2^{80} operations to find the private key) the size of an ECDSA public key would be 160 bits, whereas the size of a DSA public key is at least 1024 bits. On the other hand, the signature size is the same for both DSA and ECDSA: $4t$ bits, where t is the security level measured in bits, that is, about 320 bits for a security level of 80 bits.

4.3.2 Signature generation algorithm

Suppose Alice wants to send a signed message to Bob. Initially, they must agree on the curve parameters (CURVE, G, n) . In addition to the field and equation of the curve, we need G , a base point of prime order on the curve; n is the multiplicative order of the point G .

Alice creates a key pair, consisting of a private key integer d_A , randomly selected in the interval $[1, n-1]$; and a public key curve point $Q_A = d_A \times G$. We use $\times$ to denote elliptic curve point multiplication by a scalar.

For Alice to sign a message m , she follows these steps:

1. Calculate $e = \text{HASH}(m)$, where HASH is a cryptographic hash function, such as SHA-2.
2. Let z be the L_n leftmost bits of e , where L_n is the bit length of the group order n .
3. Select a **cryptographically secure random** integer k from $[1, n-1]$.
4. Calculate the curve point $(x_1, y_1) = k \times G$.
5. Calculate $r = x_1 \bmod n$. If $r = 0$, go back to step 3.
6. Calculate $s = k^{-1}(z + rd_A) \bmod n$. If $s = 0$, go back to step 3.
7. The signature is the pair (r, s) .

When computing s , the string z resulting from $\text{HASH}(m)$ shall be converted to an integer. Note that z can be *greater* than n but not *longer*.[1]

As the standard notes, it is crucial to select different k for different signatures, otherwise the equation in step 6 can be solved for d_A , the private key: Given two signatures (r, s) and (r, s') , employing the same unknown k for different known messages m and m' , an attacker can calculate z and z' , and since $s - s' = k^{-1}(z - z')$ (all operations in this paragraph are done modulo n) the attacker can find $k = \frac{z-z'}{s-s'}$. Since $s = k^{-1}(z + rd_A)$, the attacker can now calculate the private key $d_A = \frac{sk-z}{r}$. This implementation failure was used, for example, to extract the signing key used in the PlayStation 3 gaming-console.[2] Another way ECDSA signature may leak private keys is when k is generated by a faulty random number generator. Such a failure in random number generation caused users of Android Bitcoin Wallet to lose their funds in August 2013.[3] To ensure that k is unique for each message one may bypass random number generation completely and generate deterministic signatures by deriving k from both the message and the private key.[4]

4.3.3 Signature verification algorithm

For Bob to authenticate Alice's signature, he must have a copy of her public-key curve point Q_A . Bob can verify Q_A is a valid curve point as follows:

1. Check that Q_A is not equal to the identity element O , and its coordinates are otherwise valid

2. Check that Q_A lies on the curve
3. Check that $n \times Q_A = O$

After that, Bob follows these steps:

1. Verify that r and s are integers in $[1, n-1]$. If not, the signature is invalid.
2. Calculate $e = \text{HASH}(m)$, where HASH is the same function used in the signature generation.
3. Let z be the L_n leftmost bits of e .
4. Calculate $w = s^{-1} \bmod n$.
5. Calculate $u_1 = zw \bmod n$ and $u_2 = rw \bmod n$.
6. Calculate the curve point $(x_1, y_1) = u_1 \times G + u_2 \times Q_A$.
7. The signature is valid if $r \equiv x_1 \pmod{n}$, invalid otherwise.

Note that using Shamir's trick, a sum of two scalar multiplications $u_1 \times G + u_2 \times Q_A$ can be calculated faster than two scalar multiplications done independently.[5]

4.3.4 Correctness of the algorithm

It is not immediately obvious why verification even functions correctly. To see why, denote as C the curve point computed in step 6 of verification,

$C = u_1 \times G + u_2 \times Q_A$

From the definition of the public key as $Q_A = d_A \times G$,

$C = u_1 \times G + u_2 d_A \times G$

Because elliptic curve scalar multiplication distributes over addition,

$C = (u_1 + u_2 d_A) \times G$

Expanding the definition of u_1 and u_2 from verification step 5,

$C = (zs^{-1} + rd_A s^{-1}) \times G$

Collecting the common term s^{-1} ,

$C = (z + rd_A)s^{-1} \times G$

Expanding the definition of s from signature step 6,

$C = (z + rd_A)(z + rd_A)^{-1}(k^{-1})^{-1} \times G$

Since the inverse of an inverse is the original element, and the product of an element's inverse and the element is the identity, we are left with

$C = k \times G$

From the definition of r , this is verification step 6.

This shows only that a correctly signed message will verify correctly; many other properties are required for a secure signature algorithm.

4.3.5 Security

In December 2010, a group calling itself *fail0verflow* announced recovery of the ECDSA private key used by Sony to sign software for the PlayStation 3 game console. However, this attack only worked because Sony did not properly implement the algorithm, because k was static instead of random. As pointed out in the Signature generation algorithm Section above, this makes d_A solvable and the entire algorithm useless.[6]

On March 29, 2011, two researchers published an IACR paper[7] demonstrating that it is possible to retrieve a TLS private key of a server using OpenSSL that authenticates with Elliptic Curves DSA over a binary field via a timing attack.[8] The vulnerability was fixed in OpenSSL 1.0.0e.[9]

In August 2013, it was revealed that bugs in some implementations of the Java class SecureRandom sometimes generated collisions in the k value. As discussed above, this allowed solution of the private key, in turn allowing stealing bitcoins from the containing wallet on Android app implementations, which use Java and rely on ECDSA to authenticate transactions.[10]

This issue can be prevented by deterministic generation of *k*, as described by RFC 6979.

4.3.6 See also

- Elliptic curve cryptography
- EdDSA

4.3.7 Notes

[1] NIST FIPS 186-4, July 2013, pp. 19 and 26

[2] Console Hacking 2010 - PS3 Epic Fail, page 123–128

[3] "Android Security Vulnerability". Retrieved February 24, 2015.

[4] "RFC 6979 - Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)". Retrieved February 24, 2015.

[5] "The Double-Base Number System in Elliptic Curve Cryptography" (PDF). Retrieved 22 April 2014.

[6] Bendel, Mike (2010-12-29). "Hackers Describe PS3 Security As Epic Fail, Gain Unrestricted Access". Exophase.com. Retrieved 2011-01-05.

[7] "Cryptology ePrint Archive: Report 2011/232". Retrieved February 24, 2015.

[8] Vulnerability Note VU#536044 - OpenSSL leaks ECDSA private key through a remote timing attack

[9] "ChangeLog". OpenSSL Project. Retrieved 22 April 2014.

[10] "Android bug batters Bitcoin wallets". The Register. 12 August 2013.

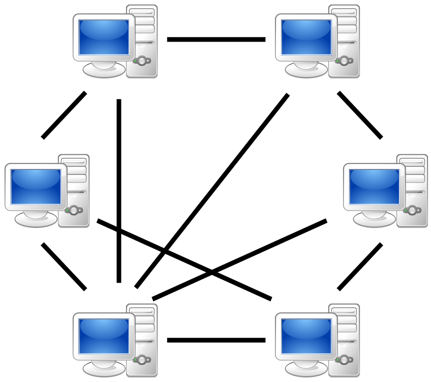
4.3.8 References

- Accredited Standards Committee X9, *American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)*, November 16, 2005.
- Certicom Research, *Standards for efficient cryptography, SEC 1: Elliptic Curve Cryptography*, Version 2.0, May 21, 2009.
- López, J. and Dahab, R. *An Overview of Elliptic Curve Cryptography*, Technical Report IC-00-10, State University of Campinas, 2000.
- Daniel J. Bernstein, Pippenger's exponentiation algorithm, 2002.
- Daniel R. L. Brown, *Generic Groups, Collision Resistance, and ECDSA*, Designs, Codes and Cryptography, **35**, 119–152, 2005. ePrint version
- Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, editors, *Advances in Elliptic Curve Cryptography*, London Mathematical Society Lecture Note Series 317, Cambridge University Press, 2005.
- Hankerson, D.; Vanstone, S.; Menezes, A. (2004). *Guide to Elliptic Curve Cryptography*. Springer Professional Computing. New York: Springer. doi:10.1007/b97644. ISBN 0-387-95273-X.

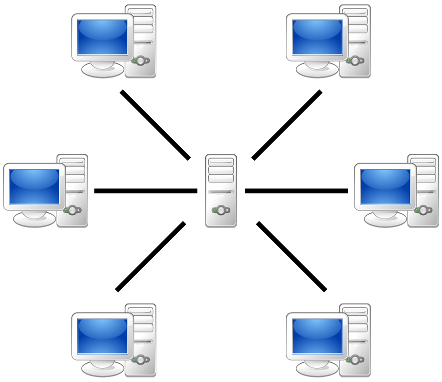
4.3.9 External links

- Digital Signature Standard; includes info on ECDSA

4.4 Peer-to-peer



*A **peer-to-peer (P2P) network** in which interconnected nodes ("peers") share resources amongst each other without the use of a centralized administrative system*



*A network based on the **client-server model**, where individual clients request services and resources from centralized servers*

Not to be confused with Point-to-point (telecommunications).

This article is about peer-to-peer computer networks. For other uses, see Peer-to-peer (disambiguation).

Peer-to-peer (**P2P**) computing or networking is a distributed application architecture that partitions tasks or work loads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.

Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.[1] Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided. Emerging collaborative P2P systems are going beyond the era of peers doing similar things while sharing resources, and are looking for diverse peers that can bring in unique resources and capabilities to a virtual community thereby empowering it to engage in greater tasks beyond those that can be accomplished by individual peers, yet that are beneficial to all the peers.[2]

While P2P systems had previously been used in many application domains,[3] the architecture was popularized by the file sharing system Napster, originally released in 1999. The concept has inspired new structures and philosophies in many areas of human interaction. In such social contexts, peer-to-peer as a meme refers to the egalitarian social networking that has emerged throughout society, enabled by Internet technologies in general.

4.4.1 Historical development

While P2P systems had previously been used in many application domains,[3] the concept was popularized by file sharing systems such as the music-sharing application Napster (originally released in 1999). The peer-to-peer movement allowed millions of Internet users to connect "directly, forming groups and collaborating to become user-created search engines, virtual supercomputers, and filesystems." [4] The basic concept of peer-to-peer computing was envisioned in earlier software systems and networking discussions, reaching back to principles stated in the first Request for Comments, RFC 1.[5]

Tim Berners-Lee's vision for the World Wide Web was close to a P2P network in that it assumed each user of the web would be an active editor and contributor, creating and linking content to form an interlinked "web" of links. The early Internet was more open than present day, where two machines connected to the Internet could send packets to each other without firewalls and other security measures.[4] This contrasts to the broadcasting-like structure of the web as it has developed over the years.[6] As a precursor to the Internet, ARPANET was a successful client-server network where "every participating node could request and serve content." However, ARPANET was not self-organized, and it lacked the ability to "provide any means for context or content-based routing beyond 'simple' address-based routing."[7]

Therefore, a distributed messaging system that is often likened as an early peer-to-peer architecture was established: USENET. USENET was developed in 1979 and is a system that enforces a decentralized model of control. The basic model is a client-server model from the user or client perspective that offers a self-organizing approach to newsgroup servers. However, news servers communicate with one another as peers to propagate Usenet news articles over the entire group of network servers. The same consideration applies to SMTP email in the sense that the core email-relaying network of mail transfer agents has a peer-to-peer character, while the periphery of e-mail clients and their direct connections is strictly a client-server relationship.

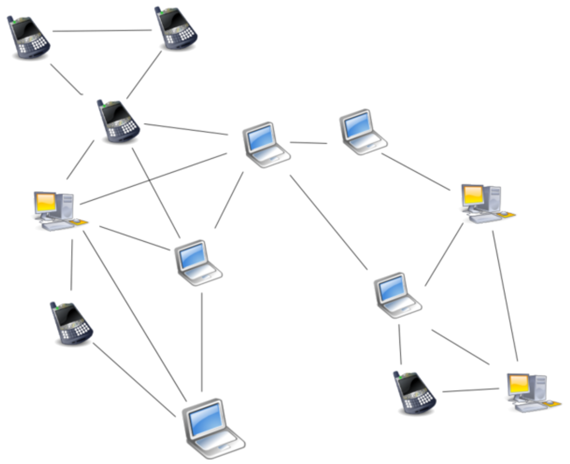
In May 1999, with millions more people on the Internet, Shawn Fanning introduced the music and file-sharing application called Napster.[7] Napster was the beginning of peer-to-peer networks, as we know them today, where "participating users establish a virtual network, entirely independent from the physical network, without having to obey any administrative authorities or restrictions."[7]

4.4.2 Architecture

A peer-to-peer network is designed around the notion of equal *peer* nodes simultaneously functioning as both "clients" and "servers" to the other nodes on the network. This model of network arrangement differs from the client–server model where communication is usually to and from a central server. A typical example of a file transfer that uses the client-server model is the File Transfer Protocol (FTP) service in which the client and server programs are distinct: the clients initiate the transfer, and the servers satisfy these requests.

Routing and resource discovery

Peer-to-peer networks generally implement some form of virtual overlay network on top of the physical network topology, where the nodes in the overlay form a subset of the nodes in the physical network. Data is still exchanged directly over the underlying TCP/IP network, but at the application layer peers are able to communicate with each other directly, via the logical overlay links (each of which corresponds to a path through the underlying physical network). Overlays are used for indexing and peer discovery, and make the P2P system independent from the physical network topology. Based on how the nodes are linked to each other within the overlay network, and how resources are indexed and located, we can classify networks as *unstructured* or *structured* (or as a hybrid between the two).[8][9][10]

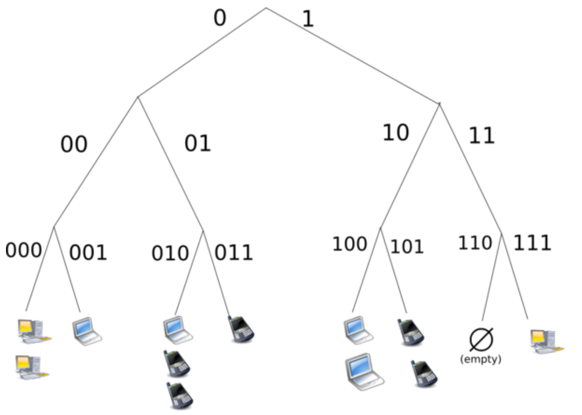


*Overlay network diagram for an **unstructured P2P network**, illustrating the ad hoc nature of the connections between nodes*

Unstructured networks *Unstructured peer-to-peer networks* do not impose a particular structure on the overlay network by design, but rather are formed by nodes that randomly form connections to each other.[11] (Gnutella, Gossip, and Kazaa are examples of unstructured P2P protocols).[12]

Because there is no structure globally imposed upon them, unstructured networks are easy to build and allow for localized optimizations to different regions of the overlay.[13] Also, because the role of all peers in the network is the same, unstructured networks are highly robust in the face of high rates of "churn"—that is, when large numbers of peers are frequently joining and leaving the network.[14][15]

However the primary limitations of unstructured networks also arise from this lack of structure. In particular, when a peer wants to find a desired piece of data in the network, the search query must be flooded through the network to find as many peers as possible that share the data. Flooding causes a very high amount of signaling traffic in the network, uses more CPU/memory (by requiring every peer to process all search queries), and does not ensure that search queries will always be resolved. Furthermore, since there is no correlation between a peer and the content managed by it, there is no guarantee that flooding will find a peer that has the desired data. Popular content is likely to be available at several peers and any peer searching for it is likely to find the same thing. But if a peer is looking for rare data shared by only a few other peers, then it is highly unlikely that search will be successful.[16]

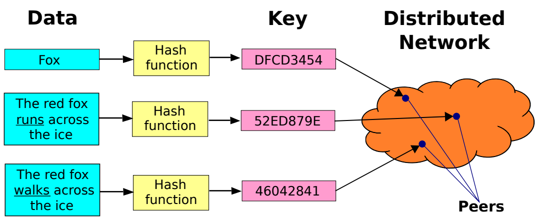


Overlay network diagram for a ***structured P2P network****, using a distributed hash table (DHT) to identify and locate nodes/resources*

Structured networks In *structured peer-to-peer networks* the overlay is organized into a specific topology, and the protocol ensures that any node can efficiently[17] search the network for a file/resource, even if the resource is extremely rare.

The most common type of structured P2P networks implement a distributed hash table (DHT),[18][19] in which a variant of consistent hashing is used to assign ownership of each file to a particular peer.[20][21] This enables peers to search for resources on the network using a hash table: that is, (*key*, *value*) pairs are stored in the DHT, and any participating node can efficiently retrieve the value associated with a given key.[22][23]

However, in order to route traffic efficiently through the network, nodes in a structured overlay must maintain lists of neighbors that satisfy specific criteria. This makes them less robust in networks with a high rate of *churn* (i.e. with large numbers of nodes frequently joining and leaving the network).[15][24] More recent evaluation of P2P resource discovery solutions under real workloads have pointed out several issues in DHT-based solutions such as high cost of advertising/discovering resources and static and dynamic load imbalance.[25]



Distributed hash tables

Notable distributed networks that use DHTs include BitTorrent's distributed tracker, the Kad network, the Storm botnet, YaCy, and the Coral Content Distribution Network. Some prominent research projects include the Chord project, Kademlia, PAST storage utility, P-Grid, a self-organized and emerging overlay network, and CoopNet content distribution system.[26] DHT-based networks have also been widely utilized for accomplishing efficient resource discovery[27][28] for grid computing systems, as it aids in resource management and scheduling of applications.

Hybrid models Hybrid models are a combination of peer-to-peer and client-server models.[29] A common hybrid model is to have a central server that helps peers find each other. Spotify is an example of a hybrid model. There are a variety of hybrid models, all of which make trade-offs between the centralized functionality provided by a structured server/client network and the node equality afforded by the pure peer-to-peer unstructured networks. Currently, hybrid models have better performance than either pure unstructured networks or pure structured networks because certain functions, such as searching, do require a centralized functionality but benefit from the decentralized aggregation of nodes provided by unstructured networks.[30]

Security and trust

Peer-to-peer systems pose unique challenges from a computer security perspective.

Like any other form of software, P2P applications can contain vulnerabilities. What makes this particularly dangerous for P2P software, however, is that peer-to-peer applications act as servers as well as clients, meaning that they can be more vulnerable to remote exploits.[31]

Routing attacks Also, since each node plays a role in routing traffic through the network, malicious users can perform a variety of "routing attacks", or denial of service attacks. Examples of common routing attacks include "incorrect lookup routing" whereby malicious nodes deliberately forward requests incorrectly or return false results, "incorrect routing updates" where malicious nodes corrupt the routing tables of neighboring nodes by sending them false information, and "incorrect routing network partition" where when new nodes are joining they bootstrap via a malicious node, which places the new node in a partition of the network that is populated by other malicious nodes.[32]

Corrupted data and malware

See also: Data validation and Malware

The prevalence of malware varies between different peer-to-peer protocols. Studies analyzing the spread of malware on P2P networks found, for example, that 63% of the answered download requests on the Limewire network contained some form of malware, whereas only 3% of the content on OpenFT contained malware. In both cases, the top three most common types of malware accounted for the large majority of cases (99% in Limewire, and 65% in OpenFT). Another study analyzing traffic on the Kazaa network found that 15% of the 500,000 file sample taken were infected by one or more of the 365 different computer viruses that were tested for.[33]

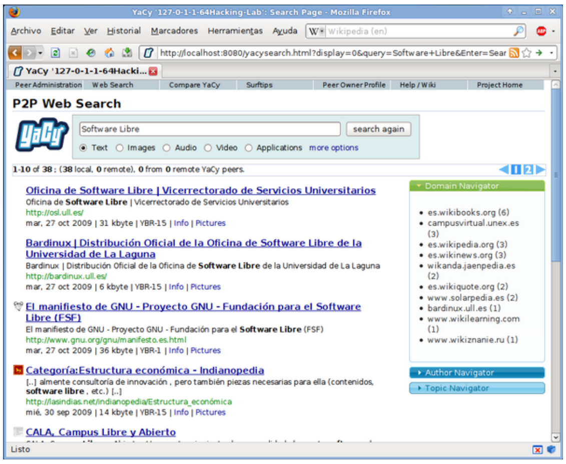
Corrupted data can also be distributed on P2P networks by modifying files that are already being shared on the network. For example, on the FastTrack network, the RIAA managed to introduce faked chunks into downloads and downloaded files (mostly MP3 files). Files infected with the RIAA virus were unusable afterwards and contained malicious code. The RIAA is also known to have uploaded fake music and movies to P2P networks in order to deter illegal file sharing.[34] Consequently, the P2P networks of today have seen an enormous increase of their security and file verification mechanisms. Modern hashing, chunk verification and different encryption methods have made most networks resistant to almost any type of attack, even when major parts of the respective network have been replaced by faked or nonfunctional hosts.[35]

Resilient and scalable computer networks

See also: Wireless mesh network and Distributed computing

The decentralized nature of P2P networks increases robustness because it removes the single point of failure that can be inherent in a client-server based system.[36] As nodes arrive and demand on the system increases, the total capacity of the system also increases, and the likelihood of failure decreases. If one peer on the network fails to function properly, the whole network is not compromised or damaged. In contrast, in a typical client–server architecture, clients share only their demands with the system, but not their resources. In this case, as more clients join the system, fewer resources are available to serve each client, and if the central server fails, the entire network is taken down.

Distributed storage and search


YaCy '127-0-1-1-64Hacking-Lab': Search Page - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Wikipedia (en)
http://localhost:8080/yacysearch.html?display=0&query=Software+Libre&Enter=Sear
YaCy '127-0-1-1-64Hacki...
Peer Administration
Web Search
Compare YaCy
Surftips
Peer Owner Profile
Help / Wiki
Project Home
search again
more options
Domain Navigator
Author Navigator
Topic Navigator
Listo

P2P Web Search

Software Libre

● Text ○ Images ○ Audio ○ Video ○ Applications

1-10 of 38 : (38 local, 0 remote), 0 from 0 remote YaCy peers.

Oficina de Software Libre | Vicerrectorado de Servicios Universitarios
Oficina de **Software Libre** | Vicerrectorado de Servicios Universitarios
http://osl.ull.es/
mar, 27 oct 2009 | 31 kbyte | YBR-15 | Info | Pictures

Bardinux | Distribución Oficial de la Oficina de Software Libre de la Universidad de La Laguna
Bardinux | Distribución Oficial de la Oficina de **Software Libre** de la Universidad de La Laguna
http://bardinux.ull.es/
mar, 27 oct 2009 | 6 kbyte | YBR-15 | Info | Pictures

El manifiesto de GNU - Proyecto GNU - Fundación para el Software Libre (FSF)
El manifiesto de GNU - Proyecto GNU - Fundación para el **Software Libre** (FSF)
http://www.gnu.org/gnu/manifesto.es.html
mar, 27 oct 2009 | 36 kbyte | YBR-1 | Info | Pictures

Categoría:Estructura económica - Indianopedia
[..] almente consultoría de innovación , pero también piezas necesarias para ella (contenidos, **software libre** , etc.) [..]
http://lasindias.net/indianopedia/Estructura_económica
mié, 30 sep 2009 | 14 kbyte | YBR-15 | Info | Pictures

CALA, Campus Libre y Abierto

- es.wikibooks.org (6)
- campusvirtual.unex.es (3)
- es.wikipedia.org (3)
- es.wikinews.org (3)
- wikanda.jaenpedia.es (2)
- es.wikiquote.org (2)
- www.solarpedia.es (2)
- bardinux.ull.es (1)
- www.wikilearning.com (1)
- www.wikiznanie.ru (1)

Search results for the query "software libre", using YaCy a free distributed search engine that runs on a peer-to-peer network instead making requests to centralized index servers (like Google, Yahoo, and other corporate search engines)

There are both advantages and disadvantages in P2P networks related to the topic of data backup, recovery, and availability. In a centralized network, the system administrators are the only forces controlling the availability of files being shared. If the administrators decide to no longer distribute a file, they simply have to remove it from their servers, and it will no longer be available to users. Along with leaving the users powerless in deciding what is distributed throughout the community, this makes the entire system vulnerable to threats and requests from the government and other large forces. For example, YouTube has been pressured by the RIAA, MPAA, and entertainment industry to filter out copyrighted content. Although server-client networks are able to monitor and manage content availability, they can have more stability in the availability of the content they choose to host. A client should not have trouble accessing obscure content that is being shared on a stable centralized network. P2P networks, however, are more unreliable in sharing unpopular files because sharing files in a P2P network requires that at least one node in the network has the requested data, and that node must be able to connect to the node requesting the data. This requirement is occasionally hard to meet because users may delete or stop sharing data at any point.[37]

In this sense, the community of users in a P2P network is completely responsible for deciding what content is available. Unpopular files will eventually disappear and become unavailable as more people stop sharing them. Popular files, however, will be highly and easily distributed. Popular files on a P2P network actually have more stability and availability than files on central networks. In a centralized network a simple loss of connection between the server and clients is enough to cause a failure, but in P2P networks the connections between every node must be lost in order to cause a data sharing failure. In a centralized system, the administrators are responsible for all data recovery and backups, while in P2P systems, each node requires its own backup system. Because of the lack of central authority in P2P networks, forces such as the recording industry, RIAA, MPAA, and the government are unable to delete or stop the sharing of content on P2P systems.[38]

4.4.3 Applications

Content delivery

In P2P networks, clients both provide and use resources. This means that unlike client-server systems, the content serving capacity of peer-to-peer networks can actually *increase* as more users begin to access the content (especially with protocols such as Bittorrent that require users to share, refer a performance measurement study[39]). This property is one of the major advantages of using P2P networks because it makes the setup and running costs very small for the original content distributor.[40][41]

File-sharing networks

Many file peer-to-peer file sharing networks, such as Gnutella, G2, and the eDonkey network popularized peer-to-peer technologies.

- Peer-to-peer content delivery networks.
- Peer-to-peer content services, e.g. caches for improved performance such as Correli Caches[42]
- Software publication and distribution (Linux distribution, several games); via file sharing networks.

Copyright infringements Peer-to-peer networking involves data transfer from one user to another without using an intermediate server. Companies developing P2P applications have been involved in numerous legal cases, primarily in the United States, over conflicts with copyright law.[43] Two major cases are *Grokster vs RIAA* and *MGM Studios, Inc. v. Grokster, Ltd.*.[44] In both of the cases the file sharing technology was ruled to be legal as long as the developers had no ability to prevent the sharing of the copyrighted material.

Multimedia

- The P2PTV and PDTP protocols.
- Some proprietary multimedia applications, such as Spotify, use a peer-to-peer network along with streaming servers to stream audio and video to their clients.
- Peercasting for multicasting streams.
- Pennsylvania State University, MIT and Simon Fraser University are carrying on a project called LionShare designed for facilitating file sharing among educational institutions globally.
- Osiris is a program that allows its users to create anonymous and autonomous web portals distributed via P2P network.

Other P2P applications

- Tradepal and M-commerce applications that power real-time marketplaces.
- Bitcoin and alternatives such as Peercoin and Nxt are peer-to-peer-based digital cryptocurrencies.
- I2P, an overlay network used to browse the Internet anonymously.
- Infinit is an unlimited and encrypted peer to peer file sharing application for digital artists written in C++.
- Netsukuku, a Wireless community network designed to be independent from the Internet.
- Dalesa, a peer-to-peer web cache for LANs (based on IP multicasting).
- Open Garden, connection sharing application that shares Internet access with other devices using Wi-Fi or Bluetooth.
- Peerspace is a peer-to-peer marketplace for booking space for events, meetings and productions.
- Research like the Chord project, the PAST storage utility, the P-Grid, and the CoopNet content distribution system.
- JXTA, a peer-to-peer protocol designed for the Java platform.
- The U.S. Department of Defense is conducting research on P2P networks as part of its modern network warfare strategy.[45] In May, 2003, Anthony Tether, then director of DARPA, testified that the United States military uses P2P networks.

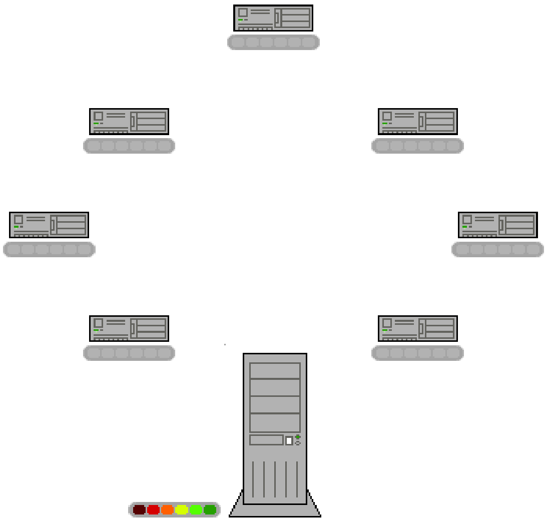
4.4.4 Social implications

See also: Social peer-to-peer processes

Incentivizing resource sharing and cooperation

Further information: Uberisation

Cooperation among a community of participants is key to the continued success of P2P systems aimed at casual human users; these reach their full potential only when large numbers of nodes contribute resources. But in current practice P2P networks often contain large numbers of users who utilize resources shared by other nodes, but who do not share anything themselves (often referred to as the "freeloader problem"). Freeloading can have a profound impact on the network and in some cases can cause the community to collapse.[46] In these types of networks "users have natural disincentives to cooperate because cooperation consumes their own resources and may degrade their own performance." [47] Studying the social attributes of P2P networks is challenging due to large populations of turnover, asymmetry of interest and zero-cost identity.[47] A variety of incentive mechanisms have been implemented to encourage or even force nodes to contribute resources.[48]



*The **BitTorrent protocol**: In this animation, the colored bars beneath all of the 7 clients in the upper region above represent the file being shared, with each color representing an individual piece of the file. After the initial pieces transfer from the seed (large system at the bottom), the pieces are individually transferred from client to client. The original seeder only needs to send out one copy of the file for all the clients to receive a copy.*

Some researchers have explored the benefits of enabling virtual communities to self-organize and introduce incentives for resource sharing and cooperation, arguing that the social aspect missing from today's P2P systems should be seen both as a goal and a means for self-organized virtual communities to be built and fostered.[49] Ongoing research efforts for designing effective incentive mechanisms in P2P systems, based on principles from game theory, are beginning to take on a more psychological and information-processing direction.

Privacy and anonymity Some peer-to-peer networks (e.g. Freenet) place a heavy emphasis on privacy and anonymity—that is, ensuring that the contents of communications are hidden from eavesdroppers, and that the identities/locations of the participants are concealed. Public key cryptography can be used to provide encryption, data validation, authorization, and authentication for data/messages. Onion routing and other mix network protocols (e.g. Tarzan) can be used to provide anonymity.[50]

4.4.5 Political implications

Intellectual property law and illegal sharing

Although peer-to-peer networks can be used for legitimate purposes, rights holders have targeted peer-to-peer over the involvement with sharing copyrighted material. Peer-to-peer networking involves data transfer from one user to another without using an intermediate server. Companies developing P2P applications have been involved in numerous legal cases, primarily in the United States, primarily over issues surrounding copyright law.[43] Two major cases are *Grokster vs RIAA* and *MGM Studios, Inc. v. Grokster, Ltd.*.[44] In both of the cases the file sharing technology was ruled to be legal as long as the developers had no ability to prevent the sharing of the copyrighted material. To establish criminal liability for the copyright infringement on peer-to-peer systems, the government must prove that the defendant infringed a copyright willingly for the purpose of personal financial gain or commercial advantage.[51] Fair use exceptions allow limited use of copyrighted material to be downloaded without acquiring permission from the rights holders. These documents are usually news reporting or under the lines of research and scholarly work. Controversies have developed over the concern of illegitimate use of peer-to-peer networks regarding public safety and national security. When a file is downloaded through a peer-to-peer network, it is impossible to know who created the file or what users are connected to the network at a given time. Trustworthiness of sources is a potential security threat that can be seen with peer-to-peer systems.[52]

Network neutrality

Peer-to-peer applications present one of the core issues in the network neutrality controversy. Internet service providers (ISPs) have been known to throttle P2P file-sharing traffic due to its high-bandwidth usage.[53] Compared to Web browsing, e-mail or many other uses of the internet, where data is only transferred in short intervals and relative small quantities, P2P file-sharing often consists of relatively heavy bandwidth usage due to ongoing file transfers and swarm/network coordination packets. In October 2007, Comcast, one of the largest broadband Internet providers in the United States, started blocking P2P applications such as BitTorrent. Their rationale was that P2P is mostly used to share illegal content, and their infrastructure is not designed for continuous, high-bandwidth traffic. Critics point out that P2P networking has legitimate legal uses, and that this is another way that large providers are trying to control use and content on the Internet, and direct people towards a client-server-based application architecture. The client-server model provides financial barriers-to-entry to small publishers and individuals, and can be less efficient for sharing large files. As a reaction to this bandwidth throttling, several P2P applications started implementing protocol obfuscation, such as the BitTorrent protocol encryption. Techniques for achieving "protocol obfuscation" involves removing otherwise easily identifiable properties of protocols, such as deterministic byte sequences and packet sizes, by making the data look as if it were random.[54] The ISP's solution to the high bandwidth is P2P caching, where an ISP stores the part of files most accessed by P2P clients in order to save access to the Internet.

4.4.6 Current research

Researchers have used computer simulations to aid in understanding and evaluating the complex behaviors of individuals within the network. "Networking research often relies on simulation in order to test and evaluate new ideas. An important requirement of this process is that results must be reproducible so that other researchers can replicate, validate, and extend existing work." [55] If the research cannot be reproduced, then the opportunity for further research is hindered. "Even though new simulators continue to be released, the research community tends towards only a handful of open-source simulators. The demand for features in simulators, as shown by our criteria and survey, is high. Therefore, the community should work together to get these features in open-source software. This would reduce the need for custom simulators, and hence increase repeatability and reputability of experiments." [55]

Besides above, there have been work done on ns-2 open source network simulator. One research issue related to free rider detection and punishment has been explored using ns-2 simulator here.[56]

4.4.7 See also

- Client–queue–client
- Cultural-Historical Activity Theory (CHAT)
- Decentralized computing
- Distributed Data Management Architecture
- Friend-to-friend
- List of P2P protocols
- Segmented downloading
- Semantic P2P networks
- Sharing economy
- Wireless ad hoc network
- USB dead drop

4.4.8 References

[1] Rüdiger Schollmeier, *A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications*, Proceedings of the First International Conference on Peer-to-Peer Computing, IEEE (2002).

[2] Bandara, H. M. N. D; A. P. Jayasumana (2012). "Collaborative Applications over Peer-to-Peer Systems – Challenges and Solutions". *Peer-to-Peer Networking and Applications*. doi:10.1007/s12083-012-0157-3.

[3] D. Barkai, *Peer-to-Peer Computing*, Intel Press, 2002.

[4] Oram, A. (Ed.). (2001). Peer-to-peer: Harnessing the Benefits of a Disruptive Technologies. O'Reilly Media, Inc.

[5] RFC 1, *Host Software*, S. Crocker, IETF Working Group (April 7, 1969)

[6] Berners-Lee, Tim (August 1996). "The World Wide Web: Past, Present and Future". Retrieved 5 November 2011. Is This "Peer-to-Peer" About? (pp. 9-16). Springer Berlin Heidelberg.

[7] Steinmetz, R., & Wehrle, K. (2005). 2. What Is This "Peer-to-Peer" About? (pp. 9-16). Springer Berlin Heidelberg.

[8] Ahson, Syed A.; Ilyas, Mohammad, eds. (2008). *SIP Handbook: Services, Technologies, and Security of Session Initiation Protocol*. Taylor & Francis. p. 204. ISBN 9781420066043.

[9] Zhu, Ce; et al., eds. (2010). *Streaming Media Architectures: Techniques and Applications: Recent Advances*. IGI Global. p. 265. ISBN 9781616928339.

[10] Kamel, Mina; et al. (2007). "Optimal Topology Design for Overlay Networks". In Akyildiz, Ian F. *Networking 2007: Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet: 6th International IFIP-TC6 Networking Conference, Atlanta, GA, USA, May 14-18, 2007 Proceedings*. Springer. p. 714. ISBN 9783540726050.

[11] Filali, Imen; et al. (2011). "A Survey of Structured P2P Systems for RDF Data Storage and Retrieval". In Hameurlain, Abdelkader; et al. *Transactions on Large-Scale Data- and Knowledge-Centered Systems III: Special Issue on Data and Knowledge Management in Grid and PSP Systems*. Springer. p. 21. ISBN 9783642230738.

[12] Zulhasnine, Mohammed; et al. (2013). "P2P Streaming Over Cellular Networks: Issues, Challenges, and Opportunities". In Pathan; et al. *Building Next-Generation Converged Networks: Theory and Practice*. CRC Press. p. 99. ISBN 9781466507616.

[13] Chervenak, Ann; Bharathi, Shishir (2008). "Peer-to-peer Approaches to Grid Resource Discovery". In Danelutto, Marco; et al. *Making Grids Work: Proceedings of the CoreGRID Workshop on Programming Models Grid and P2P System Architecture Grid Systems, Tools and Environments 12-13 June 2007, Heraklion, Crete, Greece*. Springer. p. 67. ISBN 9780387784489.

[14] Jin, Xing; Chan, S.-H. Gary (2010). "Unstructured Peer-to-Peer Network Architectures". In Shen; et al. *Handbook of Peer-to-Peer Networking*. Springer. p. 119. ISBN 978-0-387-09750-3.

[15] Lv, Qin; et al. (2002). "Can Heterogenity Make Gnutella Stable?". In Druschel, Peter; et al. *Peer-to-Peer Systems: First International Workshop, IPTPS 2002, Cambridge, MA, USA, March 7-8, 2002, Revised Papers*. Springer. p. 94. ISBN 9783540441793.

[16] Shen, Xuemin; Yu, Heather; Buford, John; Akon, Mursalin (2009). *Handbook of Peer-to-Peer Networking* (1st ed.). New York: Springer. p. 118. ISBN 0-387-09750-3.

[17] Typically approximating O(log N), where N is the number of nodes in the P2P system

[18] Other design choices include overlay rings and d-Torus. See for example Bandara, H. M. N. D.; Jayasumana, A. P. (2012). "Collaborative Applications over Peer-to-Peer Systems – Challenges and Solutions". *Peer-to-Peer Networking and Applications*. **6** (3): 257. doi:10.1007/s12083-012-0157-3.

[19] R. Ranjan, A. Harwood, and R. Buyya, "Peer-to-peer based resource discovery in global grids: a tutorial," *IEEE Commun. Surv.*, vol. 10, no. 2. and P. Trunfio, "Peer-to-Peer resource discovery in Grids: Models and systems," *Future Generation Computer Systems* archive, vol. 23, no. 7, Aug. 2007.

[20] Kelaskar, M.; Matossian, V.; Mehra, P.; Paul, D.; Parashar, M. (2002). "A Study of Discovery Mechanisms for Peer-to-Peer Application"{{inconsistent citations}}

[21] Dabek, Frank; Zhao, Ben; Druschel, Peter; Kubiatowicz, John; Stoica, Ion (2003). "Towards a Common API for Structured Peer-to-Peer Overlays". *Peer-to-Peer Systems II*. Lecture Notes in Computer Science. **2735**: 33–44. doi:10.1007/978-3-540-45172-3_3. ISBN 978-3-540-40724-9.

[22] Moni Naor and Udi Wieder. Novel Architectures for P2P Applications: the Continuous-Discrete Approach. Proc. SPAA, 2003.

[23] Gurmeet Singh Manku. Dipsea: A Modular Distributed Hash Table. Ph. D. Thesis (Stanford University), August 2004.

[24] Li, Deng; et al. (2009). Vasilakos, A.V.; et al., eds. *An Efficient, Scalable, and Robust P2P Overlay for Autonomic Communication*. Springer. p. 329. ISBN 978-0-387-09752-7.

[25] Bandara, H. M. N. Dilum; Jayasumana, Anura P. (January 2012). "Evaluation of P2P Resource Discovery Architectures Using Real-Life Multi-Attribute Resource and Query Characteristics". *IEEE Consumer Communications and Networking Conf. (CCNC '12)*.

[26] Korzun, Dmitry; Gurtov, Andrei (November 2012). *Structured P2P Systems: Fundamentals of Hierarchical Organization, Routing, Scaling, and Security*. Springer. ISBN 978-1-4614-5482-3.

[27] Ranjan, Rajiv; Harwood, Aaron; Buyya, Rajkumar (1 December 2006). "A Study on Peer-to-Peer Based Discovery of Grid Resource Information" (PDF){{inconsistent citations}}

[28] Ranjan, Rajiv; Chan, Lipo; Harwood, Aaron; Karunasekera, Shanika; Buyya, Rajkumar. "Decentralised Resource Discovery Service for Large Scale Federated Grids" (PDF).

[29] Darlagiannis, Vasilios (2005). "Hybrid Peer-to-Peer Systems". In Steinmetz, Ralf; Wehrle, Klaus. *Peer-to-Peer Systems and Applications*. Springer. ISBN 9783540291923.

[30] Yang, Beverly; Garcia-Molina, Hector (2001). "Comparing Hybrid Peer-to-Peer Systems" (PDF). *Very Large Data Bases*. Retrieved 8 October 2013.

[31] Vu, Quang H.; et al. (2010). *Peer-to-Peer Computing: Principles and Applications*. Springer. p. 8. ISBN 978-3-642-03513-5.

[32] Vu, Quang H.; et al. (2010). *Peer-to-Peer Computing: Principles and Applications*. Springer. pp. 157–159. ISBN 978-3-642-03513-5.

[33] Goebel, Jan; et al. (2007). "Measurement and Analysis of Autonomous Spreading Malware in a University Environment". In Hämmerli, Bernhard Markus; Sommer, Robin. *Detection of Intrusions and Malware, and Vulnerability Assessment: 4th International Conference, DIMVA 2007 Lucerne, Switzerland, July 12-13, 2007 Proceedings*. Springer. p. 112. ISBN 9783540736134.

[34] Sorkin, Andrew Ross (4 May 2003). "Software Bullet Is Sought to Kill Musical Piracy". New York Times. Retrieved 5 November 2011.

[35] Singh, Vivek; Gupta, Himani (2012). *Anonymous File Sharing in Peer to Peer System by Random Walks* (Technical report). SRM University. 123456789/9306.

[36] Lua, Eng Keong; Crowcroft, Jon; Pias, Marcelo; Sharma, Ravi; Lim, Steven (2005). "A survey and comparison of peer-to-peer overlay network schemes".

[37] Balakrishnan, Hari; Kaashoek, M. Frans; Karger, David; Morris, Robert; Stoica, Ion (2003). "Looking up data in P2P systems" (PDF). *Communications of the ACM*. **46** (2): 43–48. doi:10.1145/606272.606299. Retrieved 8 October 2013.

[38] "Art thou a Peer?". *www.p2pnews.net*. 14 June 2012. Retrieved 10 October 2013.

[39] Sharma P., Bhakuni A. & Kaushal R."Performance Analyis of BitTorrent Protocol. National Conference on Communications, 2013 doi:10.1109/NCC.2013.6488040

[40] Li, Jin (2008). "On peer-to-peer (P2P) content delivery" (PDF). *Peer-to-Peer Networking and Applications*. **1** (1): 45–63. doi:10.1007/s12083-007-0003-1.

[41] Stutzbach, Daniel; et al. (2005). "The scalability of swarming peer-to-peer content delivery". In Boutaba, Raouf; et al. *NETWORKING 2005 -- Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems* (PDF). Springer. pp. 15–26. ISBN 978-3-540-25809-4.

[42] Gareth Tyson, Andreas Mauthe, Sebastian Kaune, Mu Mu and Thomas Plagemann. Corelli: A Dynamic Replication Service for Supporting Latency-Dependent Content in Community Networks. In Proc. 16th ACM/SPIE Multimedia Computing and Networking Conference (MMCN), San Jose, CA (2009).

[43] Glorioso, Andrea; et al. (2010). "The Social Impact of P2P Systems". In Shen; et al. *Handbook of Peer-to-Peer Networking*. Springer. p. 48. ISBN 978-0-387-09750-3.

[44] John Borland, Judge: File-Swapping Tools are Legal , http://news.cnet.com/Judge-File-swapping-tools-are-legal/2100-1027_3-998363.html/

[45] Walker, Leslie (2001-11-08). "Uncle Sam Wants Napster!". *The Washington Post*. Retrieved 2010-05-22.

[46] Krishnan, R., Smith, M. D., Tang, Z., & Telang, R. (2004, January). The impact of free-riding on peer-to-peer networks. In System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on (pp. 10-pp). IEEE.

[47] Feldman, M., Lai, K., Stoica, I., & Chuang, J. (2004, May). Robust incentive techniques for peer-to-peer networks. In Proceedings of the 5th ACM conference on Electronic commerce (pp. 102-111). ACM.

[48] Vu, Quang H.; et al. (2010). *Peer-to-Peer Computing: Principles and Applications*. Springer. p. 172. ISBN 978-3-642-03513-5.

[49] P. Antoniadis and B. Le Grand, "Incentives for resource sharing in self-organized communities: From economics to social psychology," Digital Information Management (ICDIM '07), 2007

[50] Vu, Quang H.; et al. (2010). *Peer-to-Peer Computing: Principles and Applications*. Springer. pp. 179–181. ISBN 978-3-642-03513-5.

[51] Majoras, D. B. (2005). Peer-to-peer file-sharing technology consumer protection and competition issues. Federal Trade Commission, Retrieved from http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf

[52] The Government of the Hong Kong Special Administrative Region, (2008). Peer-to-peer network. Retrieved from website: http://www.infosec.gov.hk/english/technical/files/peer.pdf

[53] Janko Roettgers, 5 Ways to Test Whether your ISP throttles P2P, http://newteevee.com/2008/04/02/5-ways-to-test-if-your-isp-throttles-p2p/

[54] Hjelmvik, Erik; John, Wolfgang (2010-07-27). "Breaking and Improving Protocol Obfuscation" (PDF). ISSN 1652-926X.

[55] Basu, A., Fleming, S., Stanier, J., Naicken, S., Wakeman, I., & Gurbani, V. K. (2013). The state of peer-to-peer network simulators. ACM Computing Surveys, 45(4), 46.

[56] A Bhakuni, P Sharma, R Kaushal "Free-rider detection and punishment in BitTorrent based P2P networks", International Advanced Computing Conference, 2014. doi:10.1109/IAdCC.2014.6779311

4.4.9 External links

- Ghosh Debjani, Rajan Payas, Pandey Mayank P2P-VoD Streaming: Design Issues & User Experience Challenges Springer Proceedings, June 2014
- Glossary of P2P terminology
- Foundation of Peer-to-Peer Computing, Special Issue, Elsevier Journal of Computer Communication, (Ed) Javed I. Khan and Adam Wierzbicki, Volume 31, Issue 2, February 2008
- Anderson, Ross J. "The eternity service". *Pragocrypt*. **1996**.
- Marling Engle & J. I. Khan. Vulnerabilities of P2P systems and a critical look at their solutions, May 2006
- Stephanos Androutsellis-Theotokis and Diomidis Spinellis. A survey of peer-to-peer content distribution technologies. ACM Computing Surveys, 36(4):335–371, December 2004.
- Biddle, Peter, Paul England, Marcus Peinado, and Bryan Willman, The Darknet and the Future of Content Distribution. In *2002 ACM Workshop on Digital Rights Management*, November 2002.
- John F. Buford, Heather Yu, Eng Keong Lua P2P Networking and Applications. ISBN 0123742145, Morgan Kaufmann, December 2008

- Djamal-Eddine Meddour, Mubashar Mushtaq, and Toufik Ahmed, "Open Issues in P2P Multimedia Streaming", in the proceedings of the 1st Multimedia Communications Workshop MULTICOMM 2006 held in conjunction with IEEE ICC 2006 pp 43–48, June 2006, Istanbul, Turkey.
- Detlef Schoder and Kai Fischbach, "Core Concepts in Peer-to-Peer (P2P) Networking". In: Subramanian, R.; Goodman, B. (eds.): *P2P Computing: The Evolution of a Disruptive Technology*, Idea Group Inc, Hershey. 2005
- Ramesh Subramanian and Brian Goodman (eds), *Peer-to-Peer Computing: Evolution of a Disruptive Technology*, ISBN 1-59140-429-0, Idea Group Inc., Hershey, PA, United States, 2005.
- Shuman Ghosemajumder. Advanced Peer-Based Technology Business Models. *MIT Sloan School of Management, 2002.*
- Silverthorne, Sean. *Music Downloads: Pirates- or Customers?*. Harvard Business School Working Knowledge, 2004.
- Glasnost test P2P traffic shaping (Max Planck Institute for Software Systems)

4.5 Proof-of-work system

A **proof-of-work** (**POW**) **system** (or **protocol**, or **function**) is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer. The concept may have been first presented by Cynthia Dwork and Moni Naor in a 1993 journal article.[1] The term “Proof of Work” or POW was first coined and formalized in a 1999 paper by Markus Jakobsson and Ari Juels.[2]

A key feature of these schemes is their asymmetry: the work must be moderately hard (but feasible) on the requester side but easy to check for the service provider. This idea is also known as a CPU cost function, client puzzle, computational puzzle or CPU pricing function. It is distinct from a CAPTCHA, which is intended for a human to solve quickly, rather than a computer. Proof of space (PoS) proposal apply the same principle by proving a dedicated amount of memory or disk space instead of CPU time. Proof of bandwidth approaches have been discussed in the context of cryptocurrency. Proof of ownership aims at proving that specific data are held by the prover.

4.5.1 Background

One popular system—used in bitcoin mining and Hashcash— uses partial hash inversions to prove that work was done, as a good-will token to send an e-mail. For instance the following header represents about 2^{52} hash computations to send a message to calvin@comics.net on January 19, 2038:

X-Hashcash: 1:52:380119:calvin@comics.net:::9B760005E92F0DAE

It is verified with a single computation by checking that the SHA-1 hash of the stamp (omit the header name X-Hashcash: including the colon and any amount of whitespace following it) begins with 52 binary zeros, that is 13 hexadecimal zeros:^

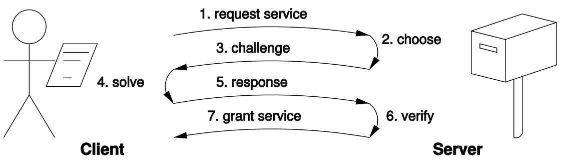
0000000000000756af69e2ffbdb930261873cd71

Whether POW systems can actually solve a particular denial-of-service issue such as the spam problem is subject to debate;[3][4] the system must make sending spam emails obtrusively unproductive for the spammer, but should also not prevent legitimate users from sending their messages. Proof-of-work systems are being used as a primitive by other more complex cryptographic systems such as bitcoin which uses a system similar to Hashcash.

4.5.2 Variants

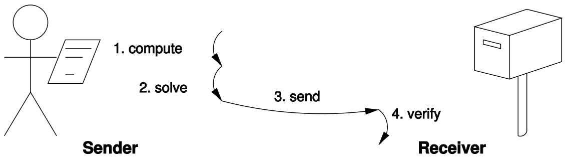
There are two classes of proof-of-work protocols.

- **Challenge-response** protocols assume a direct interactive link between the requester (client) and the provider (server). The provider chooses a challenge, say an item in a set with a property, the requester finds the relevant response in the set, which is sent back and checked by the provider. As the challenge is chosen on the spot by the provider, its difficulty can be adapted to its current load. The work on the requester side may be bounded if the challenge-response protocol has a known solution (chosen by the provider), or is known to exist within a bounded search space.



- **Solution-verification** protocols do not assume such a link: as a result the problem must be self-imposed before a solution is sought by the requester, and the provider must check both the problem choice and the found solution. Most such schemes are unbounded probabilistic iterative procedures such as Hashcash.

Known-solution protocols tend to have slightly lower variance than unbounded probabilistic protocols, because the



variance of a rectangular distribution is lower than the variance of a Poisson distribution (with the same mean). A generic technique for reducing variance is to use multiple independent sub-challenges, as the average of multiple samples will have lower variance.

There are also fixed-cost functions such as the time-lock puzzle.

Moreover, the underlying functions used by these schemes may be:

- **CPU-bound** where the computation runs at the speed of the processor, which greatly varies in time, as well as from high-end server to low-end portable devices.[5]
- **Memory-bound**[6][7][8][9] where the computation speed is bound by main memory accesses (either latency or bandwidth), the performance of which is expected to be less sensitive to hardware evolution.
- **Network-bound**[10] if the client must perform few computations, but must collect some tokens from remote servers before querying the final service provider. In this sense the work is not actually performed by the requester, but it incurs delays anyway because of the latency to get the required tokens.

Finally, some POW systems offer **shortcut** computations that allow participants who know a secret, typically a private key, to generate cheap POWs. The rationale is that mailing-list holders may generate stamps for every recipient without incurring a high cost. Whether such a feature is desirable depends on the usage scenario.

4.5.3 List of proof-of-work functions

Here is a list of known proof-of-work functions:

- Integer square root modulo a large prime[1]
- Weaken Fiat–Shamir signatures[1]
- Ong–Schnorr–Shamir signature broken by Pollard[1]
- Partial hash inversion[11][12][2] This paper formalizes the idea of a proof of work (POW) and introduces "the dependent idea of a bread pudding protocol", a "re-usable proof of work" (RPOW) system.*[13] as Hashcash*
- Hash sequences[14]
- Puzzles[15]
- Diffie–Hellman-based puzzle[16]
- Moderate[6]
- Mbound[7]
- Hokkaido[8]
- Cuckoo Cycle[9]
- Merkle tree based[17]
- Guided tour puzzle protocol[10]

4.5.4 Reusable proof-of-work as e-money

Computer scientist Hal Finney built on the proof-of-work idea, yielding a system that exploited reusable proof of work ("RPOW").[18] The idea of making proofs-of-work reusable for some practical purpose had already been established in 1999.[2] Finney's purpose for RPOW was as token money. Just as a gold coin's value is thought to be underpinned by the value of the raw gold needed to make it, the value of an RPOW token is guaranteed by the value of the real-world resources required to 'mint' a POW token. In Finney's version of RPOW, the POW token is a piece of Hashcash.

A website can demand a POW token in exchange for service. Requiring a POW token from users would inhibit frivolous or excessive use of the service, sparing the service's underlying resources, such as bandwidth to the Internet, computation, disk space, electricity and administrative overhead.

Finney's RPOW system differed from a POW system in permitting random exchange of tokens without repeating the work required to generate them. After someone had "spent" a POW token at a website, the website's operator could exchange that "spent" POW token for a new, unspent RPOW token, which could then be spent at some third party web site similarly equipped to accept RPOW tokens. This would save the resources otherwise needed to 'mint' a POW token. The anti-counterfeit property of the RPOW token was guaranteed by remote attestation. The RPOW server that exchanges a used POW or RPOW token for a new one of equal value uses remote attestation to allow any interested party to verify what software is running on the RPOW server. Since the source code for Finney's RPOW software was published (under a BSD-like license), any sufficiently knowledgeable programmer could, by inspecting the code, verify that the software (and, by extension, the RPOW server) never issued a new token except in exchange for a spent token of equal value.

Until 2009, Finney's system was the only RPOW system to have been implemented; it never saw economically significant use. In 2009, the bitcoin network went online. Bitcoin is a proof-of-work cryptocurrency that, like Finney's RPOW, is also based on the Hashcash POW. But in bitcoin double-spend protection is provided by a decentralized P2P protocol for tracking transfers of coins, rather than the hardware trusted computing function used by RPOW. Bitcoin has better trustworthiness because it is protected by computation; RPOW is protected by the private keys stored in the TPM hardware and manufacturers holding TPM private keys. Hackers who steal a TPM manufacturer key, or anyone capable of obtaining the key by examining the TPM chip itself, could subvert that assurance. Bitcoins are "mined" using the Hashcash proof-of-work function by individual nodes and verified by the decentralized P2P bitcoin network.

Other cryptocurrencies have used different hashing algorithms, as well as prime chains as proof of work.

4.5.5 Notes

1.^ On most Unix systems this can be verified with a command: echo -n 1:52:380119:calvin@comics.net:::9B760005E92F0DAE | openssl sha1

4.5.6 See also

- Bitcoin
- Cryptocurrency
- Bitmessage
- Proof-of-stake

4.5.7 References

[1] Dwork, Cynthia; Naor, Moni (1993). "Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology". *CRYPTO'92: Lecture Notes in Computer Science No. 740*. Springer: 139–147.

[2] Jakobsson, Markus; Juels, Ari (1999). "Proofs of Work and Bread Pudding Protocols". *Communications and Multimedia Security*. Kluwer Academic Publishers: 258–272.

[3] Laurie, Ben; Clayton, Richard (May 2004). "Proof-of-work proves not to work". *WEIS 04*.

[4] Liu, Debin; Camp, L. Jean (June 2006). "Proof of Work can work - Fifth Workshop on the Economics of Information Security".

[5] How powerful was the Apollo 11 computer?, a specific comparison that shows how different classes of devices have different processing power.

[6] Abadi, Martín; Burrows, Mike; Manasse, Mark; Wobber, Ted (2005). "Moderately hard, memory-bound functions". *ACM Trans. Inter. Tech.* **5** (2): 299–327.

[7] Dwork, Cynthia; Goldberg, Andrew; Naor, Moni (2003). "On memory-bound functions for fighting spam". *Advances in Cryptology: CRYPTO 2003*. Springer. **2729**: 426–444.

[8] Coelho, Fabien. "Exponential memory-bound functions for proof of work protocols". *Cryptology ePrint Archive, Report*.

[9] Tromp, John (2015). "Cuckoo Cycle; a memory bound graph-theoretic proof-of-work" (PDF). *Financial Cryptography and Data Security: BITCOIN 2015*. Springer. pp. 49–62.

[10] Abliz, Mehmud; Znati, Taieb (December 2009). "A Guided Tour Puzzle for Denial of Service Prevention". *Proceedings of the Annual Computer Security Applications Conference (ACSAC) 2009*. Honolulu, HI: 279–288.

[11] Back, Adam. "HashCash". Popular proof-of-work system. First announce in March 1997.

[12] Gabber, Eran; Jakobsson, Markus; Matias, Yossi; Mayer, Alain J. (1998). "Curbing junk e-mail via secure classification". *Financial Cryptography*: 198–213.

[13] Wang, Xiao-Feng; Reiter, Michael (May 2003). "Defending against denial-of-service attacks with puzzle auctions" (PDF). *IEEE Symposium on Security and Privacy '03*.

[14] Franklin, Matthew K.; Malkhi, Dahlia (1997). "Auditable metering with lightweight security". *Financial Cryptography '97*. Updated version May 4, 1998.

[15] Juels, Ari; Brainard, John (1999). "Client puzzles: A cryptographic defense against connection depletion attacks". *NDSS 99*.

[16] Waters, Brent; Juels, Ari; Halderman, John A.; Felten, Edward W. (2004). "New client puzzle outsourcing techniques for DoS resistance". *11th ACM Conference on Computer and Communications Security*.

[17] Coelho, Fabien. "An (almost) constant-effort solution-verification proof-of-work protocol based on Merkle trees". *Cryptology ePrint Archive, Report*.

[18] "Reusable Proofs of Work". Archived from the original on December 22, 2007.

4.5.8 External links

- Finney's system at the Wayback Machine (archived December 22, 2007)
- Bit gold. *Describes a complete money system (including generation, storage, assay, and transfer) based on proof of work functions and the machine architecture problem raised by the use of these functions.*

4.6 SHA-2

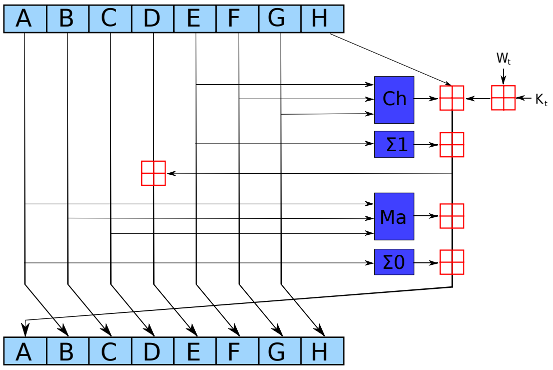
SHA-2 (**Secure Hash Algorithm 2**) is a set of cryptographic hash functions designed by the National Security Agency (NSA).[3] SHA stands for Secure Hash Algorithm. Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. For example, computing the hash of a downloaded file and comparing the result to a previously published hash result can show whether the download has been modified or tampered with.[4] A key aspect of cryptographic hash functions is their collision resistance: nobody should be able to find two different input values that result in the same hash output.

SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: **SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256**.

SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are simply truncated versions of the first two, computed with different initial values. SHA-512/224 and SHA-512/256 are also truncated versions of SHA-512, but the initial values are generated using the method described in Federal Information Processing Standards (FIPS) PUB 180-4. SHA-2 was published in 2001 by the National Institute of Standards and Technology (NIST) a U.S. federal standard (FIPS). The SHA-2 family of algorithms are patented in US patent 6829355.[5] The United States has released the patent under a royalty-free license.[6]

In 2005, an algorithm emerged for finding SHA-1 collisions in about 2,000-times fewer steps than was previously thought possible.[7] Although (as of 2015) no example of a SHA-1 collision has been published yet, the security margin left by SHA-1 is weaker than intended, and its use is therefore no longer recommended for applications that depend on collision resistance, such as digital signatures. Although SHA-2 bears some similarity to the SHA-1 algorithm, these attacks have not been successfully extended to SHA-2.

Currently, the best public attacks break preimage resistance for 52 rounds of SHA-256 or 57 rounds of SHA-512, and collision resistance for 46 rounds of SHA-256, as shown in the *Cryptanalysis and validation* section below.[1][2]



One iteration in a SHA-2 family compression function. The blue components perform the following operations:
$\mathrm{Ch}(E,F,G) = (E \wedge F) \oplus (\neg E \wedge G)$ $\mathrm{Ma}(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$ $\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$ $\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$
The bitwise rotation uses different constants for SHA-512. The given numbers are for SHA-256. The red $\boxplus$ *is addition modulo* 2^{32}.

4.6.1 Hash standard

With the publication of FIPS PUB 180-2, NIST added three additional hash functions in the SHA family. The algorithms are collectively known as SHA-2, named after their digest lengths (in bits): SHA-256, SHA-384, and SHA-512.

The algorithms were first published in 2001 in the draft FIPS PUB 180-2, at which time public review and comments were accepted. In August 2002, FIPS PUB 180-2 became the new Secure Hash Standard, replacing FIPS PUB 180-1, which was released in April 1995. The updated standard included the original SHA-1 algorithm, with updated technical notation consistent with that describing the inner workings of the SHA-2 family.[8]

In February 2004, a change notice was published for FIPS PUB 180-2, specifying an additional variant, SHA-224, defined to match the key length of two-key Triple DES.[9] In October 2008, the standard was updated in FIPS PUB 180-3, including SHA-224 from the change notice, but otherwise making no fundamental changes to the standard. The primary motivation for updating the standard was relocating security information about the hash algorithms and recommendations for their use to Special Publications 800-107 and 800-57.[10][11][12] Detailed test data and example message digests were also removed from the standard, and provided as separate documents.[13]

In January 2011, NIST published SP800-131A, which specified a move from the current minimum security of 80-bits (provided by SHA-1) allowable for federal government use until the end of 2013, with 112-bit security (provided by SHA-2) being the minimum requirement current thereafter, and the recommended security level from the publication date.[14]

In March 2012, the standard was updated in FIPS PUB 180-4, adding the hash functions SHA-512/224 and SHA-512/256, and describing a method for generating initial values for truncated versions of SHA-512. Additionally, a restriction on padding the input data prior to hash calculation was removed, allowing hash data to be calculated simultaneously with content generation, such as a real-time video or audio feed. Padding the final data block must still occur prior to hash output.[15]

In July 2012, NIST revised SP800-57, which provides guidance for cryptographic key management. The publication disallows creation of digital signatures with a hash security lower than 112-bits after 2013. The previous revision from 2007 specified the cutoff to be the end of 2010.[12] In August 2012, NIST revised SP800-107 in the same manner.[11]

The NIST hash function competition selected a new hash function, SHA-3, in 2012.[16] The SHA-3 algorithm is not derived from SHA-2.

4.6.2 Applications

For more details on this topic, see Cryptographic hash function § Applications.

The SHA-2 hash function is implemented in some widely used security applications and protocols, including TLS and SSL, PGP, SSH, S/MIME, and IPsec.

SHA-256 partakes in the process of authenticating Debian GNU/Linux software packages[17] and in the DKIM message signing standard; SHA-512 is part of a system to authenticate archival video from the International Criminal Tribunal of the Rwandan genocide.[18] SHA-256 and SHA-512 are proposed for use in DNSSEC.[19] Unix and Linux vendors are moving to using 256- and 512-bit SHA-2 for secure password hashing.[20]

Several cryptocurrencies like Bitcoin use SHA-256 for verifying transactions and calculating proof-of-work or proof-of-stake. The rise of ASIC SHA-2 accelerator chips has led to the use of scrypt-based proof-of-work schemes.

SHA-1 and SHA-2 are the secure hash algorithms required by law for use in certain U.S. Government applications, including use within other cryptographic algorithms and protocols, for the protection of sensitive unclassified information. FIPS PUB 180-1 also encouraged adoption and use of SHA-1 by private and commercial organizations. SHA-1 is being retired for most government uses; the U.S. National Institute of Standards and Technology says, "Federal agencies ***should*** stop using SHA-1 for...applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010" (emphasis in original).[21] NIST's directive that U.S. government agencies must stop uses of SHA-1 after 2010[22] was hoped to accelerate migration away from SHA-1.

The SHA-2 functions were not quickly adopted, despite better security than SHA-1. Reasons might include lack of support for SHA-2 on systems running Windows XP SP2 or older[23] and a lack of perceived urgency since SHA-1 collisions have not yet been found. The Google Chrome team announced a plan to make their web browser gradually stop honoring SHA-1-dependent TLS certificates over a period from late 2014 and early 2015.[24][25][26]

4.6.3 Cryptoanalysis and validation

For a hash function for which L is the number of bits in the message digest, finding a message that corresponds to a given message digest can always be done using a brute force search in 2^L evaluations. This is called a preimage attack and may or may not be practical depending on L and the particular computing environment. The second criterion, finding two different messages that produce the same message digest, known as a collision, requires on average only $2^{L/2}$ evaluations using a birthday attack.

Some of the applications that use cryptographic hashes, such as password storage, are only minimally affected by a collision attack. Constructing a password that works for a given account requires a preimage attack, as well as access to the hash of the original password (typically in the shadow file) which may or may not be trivial. Reversing password encryption (e.g., to obtain a password to try against a user's account elsewhere) is not made possible by the attacks. (However, even a secure password hash cannot prevent brute-force attacks on weak passwords.)

In the case of document signing, an attacker could not simply fake a signature from an existing document—the attacker would have to produce a pair of documents, one innocuous and one damaging, and get the private key holder to sign the innocuous document. There are practical circumstances in which this is possible; until the end of 2008, it was possible to create forged SSL certificates using an MD5 collision which would be accepted by widely used web browsers.[27]

Increased interest in cryptographic hash analysis during the SHA-3 competition produced several new attacks on the SHA-2 family, the best of which are given in the table below. Only the collision attacks are of practical complexity; none of the attacks extend to the full round hash function.

At FSE 2012, researchers at Sony gave a presentation suggesting pseudo-collision attacks could be extended to 52 rounds on SHA-256 and 57 rounds on SHA-512 by building upon the biclique pseudo-preimage attack.[28]

Official validation

Main article: Cryptographic Module Validation Program

Implementations of all FIPS-approved security functions can be officially validated through the CMVP program, jointly run by the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE). For informal verification, a package to generate a high number of test vectors is made available for download on the NIST site; the resulting verification, however, does not replace the formal CMVP validation, which is required by law for certain applications.

As of December 2013, there are over 1300 validated implementations of SHA-256 and over 900 of SHA-512, with only 5 of them being capable of handling messages with a length in bits not a multiple of eight while supporting both variants (see SHS Validation List).

4.6.4 Test vectors

Hash values of empty string.

SHA224("") 0x d14a028c2a3a2bc9476102bb288234c415a2b01f828ea62ac5b3e42f
SHA256("") 0x e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA384("") 0x 38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe76f65fbd51ad2f14898b95b
SHA512("") 0x cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f6
SHA512/224("") 0x 6ed0dd02806fa89e25de060c19d3ac86cabb87d6a0ddd05c333b84f4
SHA512/256("") 0x c672b8d1ef56ed28ab87c3622c5114069bdd3ad7b8f9737498d0c01ecef0967a

Even a small change in the message will (with overwhelming probability) result in a mostly different hash, due to the avalanche effect. For example, adding a period to the end of this sentence changes 111 out of 224 bits in the hash:

SHA224("The quick brown fox jumps over the lazy dog") 0x 730e109bd7a8a32b1cb9d9a09aa2325d2430587ddbc0c38bad911525
SHA224("The quick brown fox jumps over the lazy dog.”) 0x 619cba8e8e05826e9b8c519c0a5c68f4fb653e8a3d8aa04bb2c8cd4c

4.6.5 Pseudocode

Pseudocode for the SHA-256 algorithm follows. Note the great increase in mixing between bits of the w[16..63] words compared to SHA-1.

Note 1: All variables are 32 bit unsigned integers and addition is calculated modulo 2^{32} Note 2: For each round, there is one round constant k[i] and one entry in the message schedule array w[i], $0 \leq i \leq 63$ Note 3: The compression function uses 8 working variables, a through h Note 4: Big-endian convention is used when expressing the constants in this pseudocode, and when parsing message block data from bytes to words, for example, the first word of the input message “abc” after padding is 0x61626380 *Initialize hash values:* (first 32 bits of the *fractional parts* of the square roots of the first 8 primes 2..19): h0 := 0x6a09e667 h1 := 0xbb67ae85 h2 := 0x3c6ef372 h3 := 0xa54ff53a h4 := 0x510e527f h5 := 0x9b05688c h6 := 0x1f83d9ab h7 := 0x5be0cd19 *Initialize array of round constants:* (first 32 bits of the *fractional parts* of the cube roots of the first 64 primes 2..311): k[0..63] := 0x428a2f98, 0x71374491, 0xb5c0fbcf, 0xe9b5dba5, 0x3956c25b, 0x59f111f1, 0x923f82a4, 0xab1c5ed5, 0xd807aa98, 0x12835b01, 0x243185be, 0x550c7dc3, 0x72be5d74, 0x80deb1fe, 0x9bdc06a7, 0xc19bf174, 0xe49b69c1, 0xefbe4786, 0x0fc19dc6, 0x240ca1cc, 0x2de92c6f, 0x4a7484aa, 0x5cb0a9dc, 0x76f988da, 0x983e5152, 0xa831c66d, 0xb00327c8, 0xbf597fc7, 0xc6e00bf3, 0xd5a79147, 0x06ca6351, 0x14292967, 0x27b70a85, 0x2e1b2138, 0x4d2c6dfc, 0x53380d13, 0x650a7354, 0x766a0abb, 0x81c2c92e, 0x92722c85, 0xa2bfe8a1, 0xa81a664b, 0xc24b8b70, 0xc76c51a3, 0xd192e819, 0xd6990624, 0xf40e3585, 0x106aa070, 0x19a4c116, 0x1e376c08, 0x2748774c, 0x34b0bcb5, 0x391c0cb3, 0x4ed8aa4a, 0x5b9cca4f, 0x682e6ff3, 0x748f82ee, 0x78a5636f, 0x84c87814, 0x8cc70208, 0x90befffa, 0xa4506ceb, 0xbef9a3f7, 0xc67178f2 *Pre-processing:* append the bit '1' to the message append k bits '0', where k is the minimum number >= 0 such that the resulting message length (modulo 512 in *bits*) is 448. append length of message (without the '1' bit or padding), in *bits*, as 64-bit big-endian integer (this will make the entire post-processed length a multiple of 512 bits) *Process the message in successive 512-bit chunks:* break message into 512-bit chunks **for** each chunk create a 64-entry message schedule array w[0..63] of 32-bit words *(The initial values in w[0..63] don't matter, so many implementations zero them here)* copy chunk into first 16 words w[0..15] of the message schedule array *Extend the first 16 words into the remaining 48 words w[16..63] of the message schedule array:* **for** i **from** 16 to 63 s0 := (w[i-15] **rightrotate** 7) **xor** (w[i-15] **rightrotate** 18) **xor** (w[i-15] **rightshift** 3) s1 := (w[i-2] **rightrotate** 17) **xor** (w[i-2] **rightrotate** 19) **xor** (w[i-2] **rightshift** 10) w[i] := w[i-16] **+** s0 **+** w[i-7] **+** s1 *Initialize working variables to current hash value:* a := h0 b := h1 c := h2 d := h3 e := h4 f := h5 g := h6 h := h7 *Compression function main loop:* **for** i **from** 0 to 63 S1 := (e **rightrotate** 6) **xor** (e **rightrotate** 11) **xor** (e **rightrotate** 25) ch := (e **and** f) **xor** ((**not** e) **and** g) temp1 := h **+** S1 **+** ch **+** k[i] **+** w[i] S0 := (a **rightrotate** 2) **xor** (a **rightrotate** 13) **xor** (a **rightrotate** 22) maj := (a **and** b) **xor** (a **and** c) **xor** (b **and** c) temp2 := S0 **+** maj h := g g := f f := e e := d **+** temp1 d := c c := b b := a a := temp1 **+** temp2 *Add the compressed chunk to the current hash value:* h0 := h0 **+** a h1 := h1 **+** b h2 := h2 **+** c h3 := h3 **+** d h4 := h4 **+** e h5 := h5 **+** f h6 := h6 **+** g h7 := h7 **+** h *Produce the final hash value (big-endian):* digest := hash := h0 **append** h1 **append** h2 **append** h3 **append** h4 **append** h5 **append** h6 **append** h7

The computation of the ch and maj values can be optimized the same way as described for SHA-1.

SHA-224 is identical to SHA-256, except that:

- the initial hash values h0 through h7 are different, and
- the output is constructed by omitting h7.

SHA-224 initial hash values (in big endian): (The second 32 bits of the fractional parts of the square roots of the 9th through 16th primes 23..53) h[0..7] := 0xc1059ed8, 0x367cd507, 0x3070dd17, 0xf70e5939, 0xffc00b31, 0x68581511, 0x64f98fa7, 0xbefa4fa4

SHA-512 is identical in structure to SHA-256, but:

- the message is broken into 1024-bit chunks,
- the initial hash values and round constants are extended to 64 bits,
- there are 80 rounds instead of 64,
- the message schedule array w has 80 64-bit words instead of 64 32-bit words,
- to extend the message schedule array w, the loop is from 16 to 79 instead of from 16 to 63,
- the round constants are based on the first 80 primes 2..409,
- the word size used for calculations is 64 bits long,
- the appended length of the message (before pre-processing), in *bits*, is a 128-bit big-endian integer, and
- the shift and rotate amounts used are different.

SHA-512 initial hash values (in big-endian): h[0..7] := 0x6a09e667f3bcc908, 0xbb67ae8584caa73b, 0x3c6ef372fe94f82b, 0xa54ff53a5f1d36f1, 0x510e527fade682d1, 0x9b05688c2b3e6c1f, 0x1f83d9abfb41bd6b, 0x5be0cd19137e2179 SHA-512 round constants: k[0..79] := [0x428a2f98d728ae22, 0x7137449123ef65cd, 0xb5c0fbcfec4d3b2f, 0xe9b5dba58189dbbc, 0x3956c25bf348b538, 0x59f111f1b605d019, 0x923f82a4af194f9b, 0xab1c5ed5da6d8118, 0xd807aa98a3030242, 0x12835b0145706fbe, 0x243185be4ee4b28c, 0x550c7dc3d5ffb4e2, 0x72be5d74f27b896f, 0x80deb1fe3b1696b1, 0x9bdc06a725c71235, 0xc19bf174cf692694, 0xe49b69c19ef14ad2, 0xefbe4786384f25e3, 0x0fc19dc68b8cd5b5, 0x240ca1cc77ac9c65, 0x2de92c6f592b0275, 0x4a7484aa6ea6e483, 0x5cb0a9dcbd41fbd4, 0x76f988da831153b5, 0x983e5152ee66dfab, 0xa831c66d2db43210, 0xb00327c898fb213f, 0xbf597fc7beef0ee4, 0xc6e00bf33da88fc2, 0xd5a79147930aa725, 0x06ca6351e003826f, 0x142929670a0e6e70, 0x27b70a8546d22ffc, 0x2e1b21385c26c926, 0x4d2c6dfc5ac42aed, 0x53380d139d95b3df, 0x650a73548baf63de, 0x766a0abb3c77b2a8, 0x81c2c92e47edaee6, 0x92722c851482353b, 0xa2bfe8a14cf10364, 0xa81a664bbc423001, 0xc24b8b70d0f89791, 0xc76c51a30654be30, 0xd192e819d6ef5218, 0xd69906245565a910, 0xf40e35855771202a, 0x106aa07032bbd1b8, 0x19a4c116b8d2d0c8, 0x1e376c085141ab53, 0x2748774cdf8eeb99, 0x34b0bcb5e19b48a8, 0x391c0cb3c5c95a63, 0x4ed8aa4ae3418acb, 0x5b9cca4f7763e373, 0x682e6ff3d6b2b8a3, 0x748f82ee5defb2fc, 0x78a5636f43172f60, 0x84c87814a1f0ab72, 0x8cc702081a6439ec, 0x90befffa23631e28, 0xa4506cebde82bde9, 0xbef9a3f7b2c67915, 0xc67178f2e372532b, 0xca273eceea26619c, 0xd186b8c721c0c207, 0xeada7dd6cde0eb1e, 0xf57d4f7fee6ed178, 0x06f067aa72176fba, 0x0a637dc5a2c898a6, 0x113f9804bef90dae, 0x1b710b35131c471b, 0x28db77f523047d84, 0x32caab7b40c72493, 0x3c9ebe0a15c9bebc, 0x431d67c49c100d4c, 0x4cc5d4becb3e42b6, 0x597f299cfc657e2a, 0x5fcb6fab3ad6faec, 0x6c44198c4a475817] SHA-512 Sum & Sigma: S0 := (a **rightrotate** 28) **xor** (a **rightrotate** 34) **xor** (a **rightrotate** 39) S1 := (e **rightrotate** 14) **xor** (e **rightrotate** 18) **xor** (e **rightrotate** 41) s0 := (w[i-15] **rightrotate** 1) **xor** (w[i-15] **rightrotate** 8) **xor** (w[i-15] **rightshift** 7) s1 := (w[i-2] **rightrotate** 19) **xor** (w[i-2] **rightrotate** 61) **xor** (w[i-2] **rightshift** 6)

SHA-384 is identical to SHA-512, except that:

- the initial hash values h0 through h7 are different (taken from the 9th through 16th primes), and
- the output is constructed by omitting h6 and h7.

SHA-384 initial hash values (in big-endian): h[0..7] := 0xcbbb9d5dc1059ed8, 0x629a292a367cd507, 0x9159015a3070dd17, 0x152fecd8f70e5939, 0x67332667ffc00b31, 0x8eb44a8768581511, 0xdb0c2e0d64f98fa7, 0x47b5481dbefa4fa4

SHA-512/t is identical to SHA-512 except that:

- the initial hash values h0 through h7 are given by the *SHA-512/t IV generation function*,
- the output is constructed by truncating the concatenation of h0 through h7 at *t* bits,
- *t* equal to 384 is not allowed, instead SHA-384 should be used as specified, and
- *t* values 224 and 256 are especially mentioned as approved.

The *SHA-512/t IV generation function* evaluates a *modified SHA-512* on the ASCII string "SHA-512/*t*", substituted with the decimal representation of *t*. The *modified*

SHA-512 is the same as SHA-512 except its initial values h0 through h7 have each been XORed with the hexadecimal constant 0xa5a5a5a5a5a5a5a5.

C++ Implementation

```
#include <cstring> // memcpy, memset #define ROL(v, c) (((v) << (c)) | ((v) >> ((sizeof(v) * 8) - (c)))) #define ROR(v, c) (((v) >> (c)) | ((v) << ((sizeof(v) * 8) - (c)))) // len usually does not include null terminator; o1 is the most significant dword, 07 the least void __cdecl SHA256(const char *src, unsigned int len, unsigned int *o0, unsigned int *o1, unsigned int *o2, unsigned int *o3, unsigned int *o4, unsigned int *o5, unsigned int *o6, unsigned int *o7) { unsigned int h0 = 1779033703; unsigned int h1 = −1150833019; unsigned int h2 = 1013904242; unsigned int h3 = −1521486534; unsigned int h4 = 1359893119; unsigned int h5 = −1694144372; unsigned int h6 = 528734635; unsigned int h7 = 1541459225; const int k[64] = { 1116352408, 1899447441, −1245643825, −373957723, 961987163, 1508970993, −1841331548, −1424204075, −670586216, 310598401, 607225278, 1426881987, 1925078388, −2132889090, −1680079193, −1046744716, −459576895, −272742522, 264347078, 604807628, 770255983, 1249150122, 1555081692, 1996064986, −1740746414, −1473132947, −1341970488, −1084653625, −958395405, −710438585, 113926993, 338241895, 666307205, 773529912, 1294757372, 1396182291, 1695183700, 1986661051, −2117940946, −1838011259, −1564481375, −1474664885, −1035236496, −949202525, −778901479, −694614492, −200395387, 275423344, 430227734, 506948616, 659060556, 883997877, 958139571, 1322822218, 1537002063, 1747873779, 1955562222, 2024104815, −2067236844, −1933114872, −1866530822, −1538233109, −1090935817, −965641998 }; unsigned int width = (len + 63) & 0xFFFFFFC0; if (!((len + 63) & 0xFFFFFFC0)) width = 64; if ((len & 0x7F) > 0x38) width += 64; unsigned int *msg = new unsigned int[width << 2]; memset(msg, 0, width); memcpy(msg, src, len); // append 1 *((char *)msg + len) = −128; // append length in big endian *((char *)msg + width - 1) = 8 * len; *((char *)msg + width - 2) = (8 * len) >> 8; *((char *)msg + width - 3) = (8 * len) >> 16; *((char *)msg + width - 4) = (8 * len) >> 24; unsigned int w[64]; unsigned char lsb; int other, s1, offset; unsigned int value, def; unsigned int t1, t2, a, b, c, d, e, f, g, h; unsigned int blocks = width >> 6; if (blocks) { int chunk = (int)((char *)msg + 2); do { unsigned int r = 0; do // w[0] -- w[15] { // must be in big endian lsb = *(char *)(chunk + 1); other = (*(char *)chunk | (((*(char *)(chunk - 2) << 8) | *(char *)(chunk - 1)) << 8)) << 8; chunk += 4; w[r++] = lsb | other; } while (r < 0x10); unsigned int *set = &w[14]; r = 48; do // w[16] -- w[63] { value = *set; ++set; def = *(set - 14); s1 = (value >> 10) ^ ROL(value, 13) ^ ROL(value, 15); set[1] = *(set - 6) + *(set - 15) + ((def >> 3) ^ ROR(def, 7) ^ ROL(*(set - 14), 14)) + s1; --r; } while (r); a = h0; b = h1; c = h2; d = h3; e = h4; f = h5; g = h6; h = h7; offset = 0; do // SHA-256 compression function { t1 = h + *(int *)((char *)k + offset) + *(unsigned int *)((char *)w + offset) + (e & f ^ g & ~e) + (ROR(e, 6) ^ ROL(e, 7) ^ ROR(e, 11)); t2 = (a & b ^ c & (a ^ b)) + (ROR(a, 2) ^ ROL(a, 10) ^ ROR(a, 13)); h = g; g = f; f = e; e = d + t1; d = c; c = b; b = a; a = t1 + t2; offset += 4; } while (offset < 0x100); h0 += a; h1 += b; h2 += c; h3 += d; h4 += e; h5 += f; h6 += g; h7 += h; } while (!(blocks--)); } delete[] msg; *o0 = h0; *o1 = h1; *o2 = h2; *o3 = h3; *o4 = h4; *o5 = h5; *o6 = h6; *o7 = h7; }
```

4.6.6 Comparison of SHA functions

In the table below, *internal state* means the “internal hash sum” after each compression of a data block.

Further information: Merkle–Damgård construction

In the bitwise operations column, “rot” stands for rotate no carry, and “shr” stands for right logical shift. All of these algorithms employ modular addition in some fashion except for SHA-3.

The performance numbers above were for a single-threaded implementation on an AMD Opteron 8354 running at 2.2 GHz under Linux in 64-bit mode, and serve only as a rough point for general comparison. More detailed performance measurements on modern processor architectures are given in the table below.

The performance numbers labeled 'x86' were running using 32-bit code on 64-bit processors, whereas the 'x86-64' numbers are native 64-bit code. While SHA-256 is designed for 32-bit calculations, it does benefit from code optimized for 64-bit processors on the x86 architecture. 32-bit implementations of SHA-512 are significantly slower than their 64-bit counterparts. Variants of both algorithms with different output sizes will perform similarly, since the message expansion and compression functions are identical, and only the initial hash values and output sizes are different. The best implementations of MD5 and SHA-1 perform between 4.5 and 6 cycles per byte on modern processors.

Testing was performed by the University of Illinois at Chicago on their hydra8 system running an Intel Xeon E3-1275 V2 at a clock speed of 3.5 GHz, and on their hydra9 system running an AMD A10-5800K at a clock speed of 3.8 GHz.[41] The referenced cycles per byte speeds above are the median performance of an algorithm digesting a 4,096 byte message using the SUPERCOP cryptographic benchmarking software.[42] The MiB/s performance is extrapolated from the CPU clockspeed on a single core, real world performance will vary due to a variety of factors.

4.6.7 See also

- Comparison of cryptographic hash functions
- Hash-based message authentication code
- Hashcash
- International Association for Cryptologic Research (IACR)
- sha1sum (sha224sum, sha256sum, sha384sum and sha512sum) commands
- Trusted timestamping

4.6.8 References

[1] Dmitry Khovratovich, Christian Rechberger & Alexandra Savelieva (2011). "Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family" (PDF). *IACR Cryptology ePrint Archive*. 2011:286.

[2] Mario Lamberger & Florian Mendel (2011). "Higher-Order Differential Attack on Reduced SHA-256" (PDF). *IACR Cryptology ePrint Archive*. 2011:37.

[3] "On the Secure Hash Algorithm family" (PDF).

[4] "Cryptographic Hash Function". About.com. Retrieved 2014-08-18.

[5] US 6829355

[6] "Licensing Declaration for US patent 6829355.". Retrieved 2008-02-17.

[7] "Schneier on Security: Cryptanalysis of SHA-1". Schneier.com. Retrieved 2011-11-08.

[8] Federal Register Notice 02-21599, Announcing Approval of FIPS Publication 180-2

[9] "FIPS 180-2 with Change Notice 1" (PDF). *csrc.nist.gov*.

[10] Federal Register Notice E8-24743, Announcing Approval of FIPS Publication 180-3

[11] FIPS SP 800-107 Recommendation for Applications Using Approved Hash Algorithms

[12] FIPS SP 800-57 Recommendation for Key Management: Part 1: General

[13] "NIST.gov - Computer Security Division - Computer Security Resource Center".

[14] FIPS SP 800-131A Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths

[15] Federal Register Notice 2012-5400, Announcing Approval of FIPS Publication 180-4

[16] "NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition". Retrieved 24 February 2015.

[17] "Debian codebase in Google Code". Google. Archived from the original on November 7, 2011. Retrieved 2011-11-08.

[18] John Markoff, A Tool to Verify Digital Records, Even as Technology Shifts, *New York Times*, January 26, 2009

[19] RFC 5702,RFC-Editor.org

[20] Ulrich Drepper, Unix crypt with SHA-256/512

[21] National Institute on Standards and Technology Computer Security Resource Center, NIST's Policy on Hash Functions, accessed March 29, 2009.

[22] "Secure Hashing". *NIST*. Retrieved 2010-11-25.

[23] Microsoft Corporation,Overview of Windows XP Service Pack 3

[24] Chromium Blog, September 5, 2014, Gradually sunsetting SHA-1

[25] Eric Mill. "SHAAAAAAAAAAAAA". *SHAAAAAAAAAAAAA.com*.

[26] Filippo Valsorda, The Unofficial Chrome SHA1 Deprecation FAQ

[27] Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger, MD5 considered harmful today: Creating a rogue CA certificate, accessed March 29, 2009.

[28] Ji Li, Takanori Isobe and Kyoji Shibutani, Sony China Research Laboratory and Sony Corporation, Converting Meet-in-the-Middle Preimage Attack into Pseudo Collision Attack: Application to SHA-2

[29] Somitra Kumar Sanadhya & Palash Sarkar (2008). "New Collision Attacks Against Up To 24-step SHA-2" (PDF). *IACR Cryptology ePrint Archive*. 2008:270.

[30] Kazumaro Aoki; Jian Guo; Krystian Matusiewicz; Yu Sasaki & Lei Wang (2009). "Preimages for step-reduced SHA-2". *Advances in Cryptology - ASIACRYPT 2009*. Lecture Notes in Computer Science. Springer Berlin Heidelberg. **5912**: 578–597. doi:10.1007/978-3-642-10366-7_34. ISBN 978-3-642-10366-7. ISSN 0302-9743.

[31] Jian Guo; San Ling; Christian Rechberger & Huaxiong Wang (2010). "Advanced meet-in-the-middle preimage attacks: First results on full Tiger, and improved results on MD4 and SHA-2" (PDF). *Advances in Cryptology - ASIACRYPT 2010*. Lecture Notes in Computer Science. Springer Berlin Heidelberg. **6477**: 56–75. doi:10.1007/978-3-642-17373-8_4. ISBN 978-3-642-17373-8. ISSN 0302-9743.

[32] Florian Mendel; Tomislav Nad; Martin Schläffer (2013). "Improving Local Collisions: New Attacks on Reduced SHA-256". *Advances in Cryptology – EUROCRYPT 2013*. Lecture Notes in Computer Science. Springer Berlin Heidelberg. **7881**: 262–278. doi:10.1007/978-3-642-38348-9_16. ISBN 978-3-642-38348-9. ISSN 0302-9743.

[33] Maria Eichlseder and Florian Mendel and Martin Schläffer (2014). "Branching Heuristics in Differential Collision Search with Applications to SHA-512" (PDF). *IACR Cryptology ePrint Archive*. 2014:302.

[34] Christoph Dobraunig; Maria Eichlseder & Florian Mendel (2016). "Analysis of SHA-512/224 and SHA-512/256" (PDF).

[35] Found on an AMD Opteron 8354 2.2 GHz processor running 64-bit Linux[36]

[36] "Crypto++ 5.6.0 Benchmarks". Retrieved 2013-06-13.

[37] "The MD5 Message-Digest Algorithm". Retrieved 2016-04-18.

[38] "The SHAppening: freestart collisions for SHA-1". Retrieved 2015-11-05.

[39] "The Sponge Functions Corner". Retrieved 2016-01-27.

[40] "The Keccak sponge function family". Retrieved 2016-01-27.

[41] SUPERCOP Benchmarks Measurements of hash functions, indexed by machine

[42] "SUPERCOP". Retrieved 24 February 2015.

Additional reading

- Henri Gilbert, Helena Handschuh: Security Analysis of SHA-256 and Sisters. Selected Areas in Cryptography 2003: pp175–193
- "Proposed Revision of Federal Information Processing Standard (FIPS) 180, Secure Hash Standard". *Federal Register*. **59** (131): 35317–35318. 1994-07-11. Retrieved 2007-04-26.

4.6.9 External links

- Descriptions of SHA-256, SHA-384, and SHA-512 from NIST
- SHA-2 Checker – SHAChecker check your SSL compatibility for SHA-2.
- Specifications for a Secure Hash Standard (SHS) – Draft for proposed SHS (SHA-0)
- Secure Hash Standard (SHS) – Proposed SHS (SHA-0)
- CSRC Cryptographic Toolkit – Official NIST site for the Secure Hash Standard
- FIPS 180-4: Secure Hash Standard (SHS) (PDF, 1.7 MB) – Current version of the Secure Hash Standard (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512), March 2012
- Test vectors for SHA-256/384/512 from the NESSIE project
- Test vectors for SHA-1, SHA-2 from NIST site
- NIST Cryptographic Hash Project SHA-3 competition
- RFC 3874: A 224-bit One-way Hash Function: SHA-224.
- RFC 6234: US Secure Hash Algorithms SHA and SHA-based HMAC and HKDF. Contains sample C implementation.

Chapter 5

Exchanges

5.1 ANX (Hong Kong company)

ANX INTERNATIONAL (formerly known as **Asia Nexgen**[1]) is a Hong Kong-based financial technology company which operates Bitcoin exchanges and associated services, such as prepaid debit cards for which the balance is backed by Bitcoin or other fiat currencies, and mobile applications for transfer of digital assets held in the customer account.[2][3][1]

5.1.1 Sub-brands

ANX offers Debit Cards to connect digital assets with traditional payment system.

ANX offers two trading platforms and both offer 24-hour online exchange:[4]

ANXBTC.com - a user-friendly Bitcoin exchange platform for general Bitcoin trading.

ANXPRO.com - a cryptocurrency exchange platform for experienced traders.

5.1.2 History

Billed as the biggest bitcoin giveaway to date, in January 2014, ANX distributed $64,000 worth of bitcoin vouchers by tapping into Chinese cash-giving tradition.[5][6] As Chinese markets increasingly embrace online transactions and e-commerce models, the tradition of giving cash gifts of "lucky money" is transformed to convenience as more and more lucky money recipients prefer to receive their money via electronic means.

5.1.3 Company Growth

In February 28, 2014, ANX INTERNATIONAL launched the world's first Digital Assets physical retail store in Sai Ying Pun, Hong Kong.[7][8][9] It has become a digital assets exchange that operates both online and brick and mortar trading platforms.[10] For the first time, buyers can simply walk into the store, pay cash and send bitcoins to their virtual wallets, instead of buying with credit cards on online exchanges.[11]

In March 13, 2014, ANX INTERNATIONAL announced the launch of its first Digital Assets ATMs,[12][13] which was the first digital currency ATMs in Hong Kong. The machine accepts deposit of Hong Kong dollars to exchange Bitcoins.

In April 2014, ANX INTERNATIONAL launched mobile app ANX Vault on Apple App Store[14] and Google Play Store.[15] The app features high security encryption, one-time passwords, and send privilege controls. It relies on industrial strength security standards provided by the ANX platform including optical three-factor authentication. The app supports major fiat currencies and cryptocurrencies.[16] All customers funds are held in the cold storage for protection against hackers.[17] ANX INTERNATIONAL also works with an industry leading service provider of DDos protection. The multi-firewall protection is also implemented into their services. All servers are hosted in the Tier 3 compliant data center.[1]

In July 2014, ANX INTERNATIONAL introduced one of the first Bitcoin debit card that can be used worldwide at any merchant that accepts debit cards and at regular ATMs to withdraw cash.[18] The ANX card is a Bitcoin only card yet it spports 10 fiat currencies.[19] One of the largest problems that Bitcoin has is that Bitcoin is not widely accepted; users want to use it have to exchange for fiat currencies. ANX has basically eliminated the problem with its Bitcoin debit card that allows users to use Bitcoins within the traditional credit card payment system.[20] Users can reload funds to the debit cards using Bitcoin. The card can be used for both online and Point of Sale purchases as well as withdrawals through the Global AT&T Network, in other words, they can easily spend their bitcoins at many locations that take traditional debit cards.[21]

In July 2014, ANX INTERNATIONAL has launched the ANX Vault that allowed to sending and receiving functionality for the Apple App Store and Google Play Store.[22] iOS users who make sure of ANX services will be able to conduct their digital assets sending/ receiving business, in addition to being able to send bitcoin by email.[22] For the security features, both versions of the app support optional three-factor authentication, although it still allows fast transactions, the app allows users to set daily spending limits that bypass the security feature.[23] ANX digital assets exchange said that other security features include the ability to disable sending privileges from a user's desktop account in the event of a lost mobile device, OTP (one-time password) support for logging in and sending funds, and 'industry standard' encryption for all data communication.[23]

5.1.4 Acquisitions

In November 2014, Hong Kong-based exchange ANX INTERNATIONAL has expanded its global presence with the acquisition of Norwegian exchange [24] Justcoin, expanding its presence in the European Bitcoin Market.[25] Justcoin was moving to run on ANX infrastructure as well as incorporating features available on ANX[25] and customers of Justcoin can trade Ripple and Stellar using the ANX order book powered by ANX's latest technology. ANX said that it was able to migrate the Justcoin platform in "less than a week" with the ANX proprietary trading engine and white-label capabilities.[26]

In January 2015, ANX announced that it required CoinMkt, the Santa Monica-based cryptocurrency exchange.[27] The acquisition will help ANX to expand the footprint in the America.[27] Whereas ANX is focused in Asia, the CoinMkt is focused in the US. ANX will have a wide of reach to cater the requirements from clients or customers.[27] CoinMkt will continue to operate under its original brand, but reside under the umbrella of ANX.[28]

5.1.5 Agreements

In December 2014, the Payment Processing specialist Vogogo signed an agreement with ANXPRO and The Rock Trading Company of Malta, a Maltese-based exchanges.[29] Rock Trading and ANXPRO will be integrated with Vogogo's payment processing and risk management platform enable each to offer users of their respective platform's seamless transactions between Bitcoin and fiat currencies in the US, Canada and the European Union. The ability to conduct transactions with traditional banks has been a major hurdle for companies of crypto-currencies to date and is seen by critical to the widespread adoption and proliferation of virtual currencies.[29] With Vogogo providing sophisticated risk management and compliance, exchanges like these have the freedom to focus on its technology and building its respective business.[29]

In January 2015, ANX added "Black Gold" Coin, which was launched by National Aten Coin.[30] Clients in National Aten Coin (NAC) will have instant access to ANXPRO's simple and user friendly UI, consolidated shared order book for blended multi-currency settlement, real time FX pricing, deposit options and risk management and trading tools.[31]

5.1.6 References

[1] "ANXBTC". *BestCoinExchange*. Retrieved 29 May 2015.

[2] Lee, Danny (2014-01-29). "Company offers bitcoin instead of cash in lai see packets". *SCMP*.

[3] "Hong Kong Bitcoin Exchange ANX Issues Bitcoin Debit Card". Cryptocoins News. 10 July 2014. Retrieved 29 May 2015.

[4] "Top 10 Best Bitcoin Exchanges". *BestCoinExchange*. Retrieved 29 May 2015.

[5] "E-commerce trumps tradition as Lunar New Year 'lucky money' goes online" (30 January 2014). CNN. Retrieved 1 June 2015.

[6] "HK$500,000 lai see giveaway... in Bitcoin". SCMP. 29 January 2014. Retrieved 1 June 2015.

[7] "A Look at the World's First Bitcoin Shop". Bloomberg. 28 February 2014. Retrieved 1 June 2015.

[8] "Bitcoin ATMs Open in Singapore". The Wall Street Journal. 28 February 2014. Retrieved 1 June 2015.

[9] "'World's first' Bitcoin shop opens doors in Hong Kong". THE STRAITS TIMES. 28 February 2015. Retrieved 26 May 2015.

[10] "Bitcoin exchange opens in Hong Kong". CNN. 3 March 2014. Retrieved 1 June 2015.

[11] Business Insider (28 February 2014). "Bitcoin Trade Volume Soars In China Following The Fall Of Mt. Gox". Business Insider. Retrieved 1 June 2015.

[12] "Hong Kong Company Launches City's First Bitcoin ATM". *International Business Times*. Retrieved 1 June 2015.

[13] "Three companies set to launch bitcoin ATMs in Hong Kong within days". South China Morning Post. Christy Choi. 14 March 2014. Retrieved 26 May 2015.

[14] "ANX Vault: Your Bitcoin Wallet". *iTunes*. Retrieved 1 June 2015.

[15] "ANX Vault: Your Bitcoin Wallet". *Google Play*. Retrieved 1 June 2015.

[16] "ANX Vault App For iOS Enables Send/Receive Functionality". NEWSBTC. 29 July 2014. Retrieved 1 June 2015.

[17] "How to prevent bitcoin hacking". CNBC. 16 February 2014. Retrieved 1 June 2015.

[18] "Hong Kong Exchange ANX Launches Bitcoin Debit Card". *CoinDesk*. July 15, 2014. Retrieved May 30, 2015.

[19] "ANX Issues World's First Bitcoin Debit Card". *CoinTelegraph*. July 13, 2014. Retrieved May 30, 2015.

[20] “ANX Issues World’s First Bitcoin Debit Card”. CoinTelegraph. 13 July 2014. Retrieved 1 June 2015.

[21] “Keiser Report: (Dis-)harmony with Cash (E702)". *Youtube*. RT Keiser Report. Retrieved 1 June 2015.

[22] “ANX Vault App For iOS Enables Send/Receive Functionality”. *NEWSBTC*. Retrieved 31 July 2015.

[23] “Bitcoin Exchange ANX Adds Features to iOS and Android Apps”. *CoinDesk*. Retrieved 31 July 2015.

[24] “Bitcoin Weekly 2015 January 28: All about exchange-Winklevoss Gemini, Coinbase Exchange, CoinMkt”. *siliconANGLE*. Retrieved 10 July 2015.

[25] “ANX Acquires Justcoin, Incorporates Platform within a Week”. THE COINTELEGRAPH. William Suberg. 21 November 2014. Retrieved 27 May 2015.

[26] “ANX Acquisition Revives Troubled Bitcoin Exchange Justcoin”. CoinDesk. Nermin Hajdarbegovic. 21 November 2014. Retrieved 27 May 2015.

[27] “Bitcoin Company ANXBTC Acquires Santa Monica-based exchange West Orange Labs, Inc”. *FareXMinute*. Retrieved 10 July 2015.

[28] “Bitcoin Weekly 2015 January 28: All about exchanges-Winklevoss Gemini, Coinbase Exchange, CoinMkt”. *siliconANGLE*. Retrieved 10 July 2015.

[29] “Bitcoin Exchange ANXPRO and Rock Trading Integrate with Vogogo”. *MarketWatch*. MarketWatch. Retrieved 27 May 2015.

[30] ""Anti-Money Laundering Coin” to Become Available for Trade on ANXPRO”. Finance Magnates. Leon Pick. 29 May 2015. Retrieved 29 May 2015.

[31] “ANXPRO Exchange to Include Aten “Black Gold” Coin in 2015”. FORWARD GEEK. Geeks News Desk. 26 January 2015. Retrieved 29 May 2015.

5.2 BitInstant

BitInstant was a bitcoin exchange start-up based in New York City.[1][2] Founded in 2011 by Gareth Nelson and Charlie Shrem, BitInstant provided a means to rapidly pay traditional funds to bitcoin exchanges.[3] As of January 2014, BitInstant’s website is no longer available, displaying only a blank page.[1] Its blog, at was unavailable as of October 31, 2014.

5.2.1 History

BitInstant was founded in 2011 by Gareth Nelson and Charlie Shrem.[3] The company allowed its customers to purchase the bitcoins via more than 700,000 stores, including Walmart, Walgreens, and Duane Reade.[4]

In September 2012, when presidential candidate Mitt Romney was threatened with blackmail unless he paid an anonymous group $1 million in bitcoin, BitInstant’s Erik Voorhees offered to purchase the bitcoin for him without a fee.[5]

According to Shrem, transaction volume grew rapidly during 2013 as the price of bitcoin rose, and “basically tripled” during April.[6]

As of May 2013, BitInstant had 16 employees when Winklevoss Capital invested $1.5 million in the company.[2] According to the Winklevosses, the funding is “meant to allow the company to further scale up its staff and product.” BitInstant later announced a partnership with the Winklevosses’ bitcoin investment fund.[7]

In June 2013, BitInstant announced integration with Jumio, an online payment company led by Daniel Mattes. Jumio’s Netverify software allows BitInstant to verify customers’ identity.[8] BitInstant also restricted bitcoin transactions in some states, stating that “We have temporarily limited transactions in some locations, and we apologize for the inconvenience. We believe that these measures are vital to serving the interests of both BitInstant and the greater bitcoin community.”.[9]

In July 2013, BitInstant suspended services, saying it wanted “to improve the code based on trends they noticed” in nearly 17,300 customer service complaints.[10] Several days earlier, a class action lawsuit had been filed on behalf of customers, claiming failure to perform services and false representation.[11]

On January 27, 2014, company CEO Charlie Shrem was arrested at New York’s JFK airport and charged with “conspiring to commit money laundering by selling more than $1 million in bitcoins to users of the black market website Silk Road...”.[12] BitInstant website has been blank since then.

5.2.2 Criticism

BitInstant received many complaints from customers concerning transaction processing delays sometimes of several days.[6][13] In response to complaints, BitInstant CTO Gareth Nelson stated that “we are all stressing out and working day and night (literally) to get things fixed and hope to have a proper resolution for the backlogged orders”.[13]

The New York State Department of Financial Services issued a warning letter to BitInstant, asking it to comply with regulations governing money transmission businesses.[14]

5.2.3 References

[1] Lee, Timothy B. “Feds charge Bitcoin start-up founder with money laundering”. Washingtonpost.com. Retrieved 2014-01-28.

[2] Taylor, Colleen (17 May 2013). "With $1.5M Led By Winklevoss Capital, BitInstant Aims To Be The Go-To Site To Buy And Sell Bitcoins". *TechCrunch*. Retrieved 11 July 2013.

[3] Emily Spaven (2013-08-15). "Frustrated customers hit BitInstant with a class action lawsuit". Coindesk.com. Retrieved 2014-01-07.

[4] Alexa Simon (2013-04-10). "Meet the Bitcoin Millionaires". Businessweek. Retrieved 2014-01-28.

[5] Garver, Abe (7 September 2012). "BitInstant To Romney Camp: 'We'll Convert $1,000,000 USD to Bitcoin For Free.'". *Forbes*. Retrieved 12 July 2013.

[6] Roose, Kevin (8 April 2013). "Inside the Bitcoin Bubble: A Q&A With BitInstant's Stressed-Out CEO". *New York Magazine*. Retrieved 11 July 2013.

[7] Gilson, David (8 July 2013). "BitInstant to partner up with Winklevoss twins' bitcoin fund". *CoinDesk*. Retrieved 11 July 2013.

[8] Jumio June 13, 2013 8:00 AM (2013-06-13). "Bitcoin Purchase Platform BitInstant Integrates Jumio's Netverify to Speed Transactions and Reduce Fraud - Yahoo Finance". Finance.yahoo.com. Retrieved 2014-01-07.

[9] "Squarespace - Account Not Available". Blog.bitinstant.com. Retrieved 2014-01-07.

[10] "BitInstant website". 15 July 2013. Retrieved 29 July 2013.

[11] *Iacono et al. v. BitInstant LLC*, Case 1:13-cv-04674-CM (S.D.N.Y. 8 July 2013).

[12] "Bitcoin Operators Charged in Illicit Drug Site Bust". Associated Press. Retrieved 27 January 2014.

[13] Siluk, Shirley (13 June 2013). "BitInstant complaints flare up after beta site launch". *CoinDesk*. Retrieved 11 July 2013.

[14] Sidel, Robin (25 June 2013). "States Put Heat on Bitcoin". *The Wall Street Journal*. Retrieved 11 July 2013.

5.2.4 External links

- Bitcoin Debit Card

5.3 Bitstamp

Bitstamp is a bitcoin exchange based in Luxembourg. As of 2016 it was the world's second largest by volume.[2] It allows trading between USD currency and bitcoin cryptocurrency. It allows USD, EUR, bitcoin or Ripple deposits and withdrawals. The company is headed by CEO Nejc Kodrič, a widely known member of the bitcoin community, who co-founded the company in August 2011 with Damijan Merlak.[1] in his native Slovenia, but later moved its registration to the UK in April 2013, then to Luxembourg in 2016.[1][nb 1]

The company was founded as a European-focused alternative to then-dominant bitcoin exchange Mt. Gox.[1] While the company trades in US dollars, it allows money to be deposited through the European Union's Single Euro Payments Area, allowing a relatively quick, low cost way of transferring money from European bank accounts to purchase bitcoins.[1]

When incorporating in the United Kingdom, the company approached the UK's Financial Conduct Authority for guidance, but was told that bitcoin was not classed as a currency, so the exchange was not subject to regulation.[1] Bitstamp says that it instead regulates itself, following a set of best practices to authenticate customers and deter money laundering.[1] In September 2013, the company began requiring account holders to verify their identity with copies of their passports and official records of their home address.[1] In 2016 the Luxembourgish government granted a license to Bitstamp to be fully regulated in the EU. The license is usable around the 28 member states of the EU. This will help the industry become more secure, robust and transparent.

Bitstamp offers an API to allow clients to use custom software to access and control their accounts.[3]

Bitstamp also acts as a gateway for the Ripple payment protocol.

5.3.1 Service disruptions

In February 2014, the company suspended withdrawals for several days in the face of a distributed denial-of-service.[4] *Bitcoin Magazine* reported that people behind the attack sent a ransom demand of 75 bitcoins to Kodrič, who refused due to a company policy against negotiating with "terrorists".[5] Days after restoring service, Bitstamp temporarily suspended withdrawals for some users as a security precaution due to increased phishing attempts.[6]

In January 2015, Bitstamp suspended its service after a hack during which less than 19,000 bitcoins were stolen.[7]

5.3.2 Notes

[1] The company is registered in Reading in the UK, but this is in fact just the offices of UK PLC, a company specialising in company formation and which, amongst its services, allows companies to use its own address as their registered office, effectively acting as a forwarding address. There is no clear information available as to where Bitstamp's operations are located or whether they actually have any presence at all in the UK, or are still run out of Slovenia.

5.3.3 References

[1] Boase, Richard; Spaven, Emily (2013-11-22). “Bitstamp shows higher Bitcoin price than Mt. Gox”. *CoinDesk*.

[2] “Bitcoin markets”. Bitcoin Charts. Retrieved September 25, 2014.

[3] “API – Bitstamp”. Bitstamp. Retrieved 2014-02-21.

[4] Spaven, Emily (2014-02-14). “Bitstamp to resume Bitcoin withdrawals today, BTC-e still working on a solution”. *CoinDesk*. Retrieved 2014-02-19.

[5] Alisie, Mihai (2012-10-15). “Bitstamp under DDoS”. *Bitcoin Magazine*. Retrieved 2014-02-21.

[6] Hajdarbegovic, Nermin (2014-02-20). “Bitstamp restores withdrawals following security scare”. *CoinDesk*. Retrieved 2014-02-21.

[7] Zack Whittaker (5 January 2015). “Bitstamp exchange hacked, $5M worth of bitcoin stolen”. *Zdnet*. CBS Interactive. Retrieved 6 January 2015.

5.3.4 External links

- Official website

5.4 BTC-e

BTC-e is a digital currency trading platform and exchange.[1] It was founded in July 2011 and as of February 2015 handles around 2.5% of all Bitcoin exchange volume.[2] It allows trading between the U. S. dollar, Russian ruble and euro currencies, and the bitcoin, litecoin, namecoin, novacoin, peercoin, dash and ethereum cryptocurrencies.

It has been a component of the CoinDesk *Bitcoin Price Index* since the index started in September 2013.[3]

Neither the names of the management, the name of the company nor the jurisdiction of incorporation are known.

5.4.1 History

BTC-e started in July 2011, handling just a few coin pairs, including Bitcoin/U. S. dollar and I0Coin to Bitcoin. By October 2011, they supported many different currency pairs, including Litecoin to dollars, Bitcoin to rubles and RuCoin to rubles.[4]

On July 31, 2012, BTC-e had their Liberty Reserve API Key compromised, the attacker injected thousands of fake U. S. dollars into the site and used it to disrupt the markets. A large amount of Bitcoins were taken during the attack, some sources estimate the equivalent of $35,000 were taken in Bitcoins. The attackers are still unknown, although BTC-e recovered without taking coins from their users.

During 2013 and 2014, BTC-e had many outages related to Distributed Denial of Service attacks.[5] They later began using the reverse proxy service CloudFlare to help mitigate these attacks, reducing downtime for the exchange.

5.4.2 References

[1] Benjamin Guttmann (2014). “The Bitcoin Bible Gold Edition”. Books on Demand. pp. 175–176. ISBN 9783732296965.

[2] “Bitcoin Exchanges Market Share”. Bitcoinity. Retrieved 2015-02-10.

[3] Del Rey, Jason (September 11, 2013). “What’s a Bitcoin Really Worth? CoinDesk Thinks It Has the Answer.”. All Things D.

[4] BTC-e (2011-10-25). “Start trading on a pairs of BTC/RUB, LTC/USD, RUC/RUB, USD/RUB!". Retrieved 2015-11-20.

[5] Jonathon Millet @ NewsBTC. “BTC-e Reports DDOS Attack Against Their Server”.

- “The Bitcoin Bible Gold Edition”. *google.com*.
- “BTC-e Pulls Support for Ruble As Russia Bans Bitcoin”. *CoinDesk*.
- “BTC-e Empowers Veteran Investors with Advanced PAMM Trading Account”. *CoinDesk*.
- “BTC-e Back Online Following DDoS Attack”. *CoinDesk*.
- Digiconomist. “Exchange Review: BTC-e”. *Digiconomist*.
- “BTC-e - Terrorist or Freedom Fighter?". *The Merkle*.
- “Bitcoin exchange BTC-e, a Mt. Gox alternative, is an Internet black hole”. *Marketwatch*.

5.5 BTC China

BTCChina, based in Shanghai, China, is the world’s second largest bitcoin exchange by volume as of October 2014.[1] Founded in June 2011, it was the China’s first bitcoin exchange, and most of its customers are thought to be Chinese.[2] In November 2013, the company had grown to 20 employees.[2]

5.5.1 History

Company CEO Bobby Lee approached the then two-person company in early 2013, and after investing his own money and attracting investors, oversaw the company's rapid expansion and marketshare growth by the end of the year.[2] The Stanford computer science graduate, whose brother founded the cryptocurrency Litecoin, previously worked for Yahoo! in the United States, and for Walmart China as Vice President of Technology.[2]

In November 2013, BTCChina raised $5 million in Series A funding from investors Lightspeed China Partners and Lightspeed Venture Partners.[3]

On 18 December 2013, BTCChina announced that it was temporarily suspending acceptance of Chinese yuan deposits, attributing the decision to government regulations, following a 5 December statement from the People's Bank of China (PBOC).[4] On 30 January 2014, the exchange resumed accepting yuan deposits, after further studying the PBOC statement and other rules.[5] While the PBOC prohibited banks from trading in Bitcoin, BTCChina explained that they were accepting yuan into their corporate bank account, and transferring that money to their customer accounts, before it was traded for bitcoins.[5]

5.5.2 References

[1] "Bitcoin Market". Bitcoin Charts. Retrieved October 10, 2014.

[2] Hill, Kashmir (2013-11-08). "From Walmart To Bitcoin: The CEO Behind The Chinese Exchange Sending BTC To New Highs". *Forbes*. Retrieved 2013-11-08.

[3] Lomas, Natasha (2013-11-18). "As Chinese Investors Pile Into Bitcoin, China's Oldest Exchange, BTCChina, Raises $5M From Lightspeed". TechCrunch. Retrieved 2014-02-21.

[4] Rose, Adam (2013-12-18). "China tightens curbs on bitcoin trade". *Reuters*. Retrieved 2014-02-21.

[5] Casey, Michael J. (2014-01-31). "China Bitcoin exchange restores deposit facility". *The Wall Street Journal*. Retrieved 2014-03-03.

5.5.3 External links

- Official site

5.6 Buttercoin

Warning: Page using Template:Infobox company with unknown parameter "Former type" (this message is shown only in preview).

Buttercoin was a private American start-up company that provided digital currency exchange services to the US.[2][3] Specifically, Buttercoin operated a full order book trading platform for buying and selling bitcoins.

On April 6, 2015, citing a loss of interest in bitcoin from venture capital firms, the company announced that it was shutting down as of April 10, 2015.[5]

5.6.1 Funding

Y Combinator, Google Ventures (Kevin Rose and Chris Hutchins), Floodate, Initialized Capital, Rothenberg Ventures, and Reddit co-founder Alexis Ohanian invested approximately $1 million into Buttercoin.[1][4] A Swiss company, Centralway Ventures, invested an additional $250,000 into Buttercoin.[3] Combined with other sources, Buttercoin raised a total of $1.6 million as of September 2013.[3] Subsequently, Buttercoin raised an undisclosed sum from Wedbush Securities, making it the first bitcoin company to receive investment from a large Wall Street institution. [6]

5.6.2 References

[1] Cutler, Kim-Mai (August 20, 2013). "YC-Backed Buttercoin Uses Bitcoin To Attack The $500B-A-Year Remittances Economy". *TechCrunch*. Retrieved November 30, 2013.

[2] Reutzel, Bailey (September 9, 2013). "Buttercoin Takes a Different Path to Handling Virtual Currency". *PaymentsSource*. Retrieved November 30, 2013.

[3] Lomas, Natasha (September 18, 2013). "Swiss Company-Builder Centralway Opens $50M Fund, Invests $250k In Bitcoin Whitelabel Exchange Buttercoin". *TechCrunch*. Retrieved December 1, 2013.

[4] Kolodny, Lora (August 19, 2013). "International Bitcoin Exchange Buttercoin Raises $1M to Revamp Remittance". *VentureWire*. Retrieved November 30, 2013. (subscription required (help)).

[5] Russell, Jon (April 6, 2015). "Google Ventures-Backed Bitcoin Exchange Buttercoin Is Shutting Down". *TechCrunch*. Retrieved April 6, 2015.

[6] Kharif, Olga (November 17, 2014). "Bitcoin Startup Buttercoin Draws Wedbush as Investor". "Bloomberg". Retrieved December 9, 2014.

5.6.3 External links

- Buttercoin Official website

5.7 Coinbase

Coinbase is a digital asset exchange company headquartered in San Francisco, California. It operates exchanges of bitcoin, Ethereum and other digital assets with fiat currencies in 32 countries, and bitcoin transactions and storage in 190 countries worldwide. [5][6][7][8]

5.7.1 History

Coinbase was founded in June 2012 by Brian Armstrong and Fred Ehrsam.[3][9] It enrolled in the summer 2012 Y Combinator startup incubator program. In October 2012 the company launched the services to buy and sell bitcoin through bank transfers.[10]

In May 2013, the company received a US$5 million Series A investment led by Fred Wilson from the venture capital firm Union Square Ventures.[11] In December 2013, the company received a US$25 million investment, from the venture capital firms Andreessen Horowitz, Union Square Ventures and Ribbit Capital.[12]

In 2014 the company grew to one million users, acquired the blockchain explorer service Blockr and the web bookmarking company Kippt, secured insurance covering the value of bitcoin stored on their servers, and launched the vault system for secure bitcoin storage.[13][14][15] Throughout 2014 the company also formed partnerships with Overstock, Dell, Expedia, Dish Network, Time Inc., and Wikipedia to power accepting bitcoin payments.[16][17][18][19][20] The company also added bitcoin payment processing capabilities to the traditional payment companies Stripe, Braintree, and PayPal.[21]

In January 2015, the company received a US$75 million investment, led by Draper Fisher Jurvetson, the New York Stock Exchange, USAA, and several banks, "apparently the first time any traditional financial institutions have taken direct stakes in a bitcoin enterprise."[22] Later in January the company launched a U.S.-based bitcoin exchange for professional traders called Coinbase Exchange.[23]

Coinbase began to offer services in Canada in 2015, but in July 2016 announced it would halt services in August after the closure of their Canadian online payments service provider Vogogo.[24]

On 29 March 2016, Coinbase was listed by UK-based company Richtopia at number 2 in the list of 100 Most Influential Blockchain Organisations.[25][26]

In May 2016, the company rebranded the Coinbase Exchange, changing the name to the Global Digital Asset Exchange (GDAX) and offering Ether, the value token of Ethereum, for trade on its professional trading exchange service.[27] In July 2016, they extended the support to their "Coinbase" retail exchange by adding Ether as only the second digital currency offered to retail customers.[28]

5.7.2 Products

Coinbase has two core products: a Global Digital Asset Exchange (GDAX) for trading a variety of digital assets on its professional asset trading platform, and a user-facing retail exchange of bitcoin and Ether for fiat currency.[28] It also offers an API for developers and merchants to build applications and accept payments in both digital currencies. As of 2014, the company offered buy/sell trading functionality in 25 countries, while the wallet was available in 190 countries worldwide.[29]

The exchange can be funded through a bank transfer or wire, and trades on the exchange have a maker/taker price model in which traders pay either a 0.25% fee (taker) or nothing (maker) to execute trades.[30]

5.7.3 See also

- Bitcoin
- Xapo
- BitPay
- Blockchain
- Uphold
- Circle (company)
- List of bitcoin companies

5.7.4 References

[1] Nermin Hajdarbegovic (2013-12-19). "Coinbase passes 650,000 users in less than a year". *CoinDesk*. Retrieved 2014-01-10.

[2] "About Coinbase". Coinbase. Retrieved 1 Oct 2014.

[3] "Company Overview of Coinbase, Inc.". Bloomberg News. Retrieved 1 July 2014.

[4] "Coinbase". LinkedIn. Retrieved 1 July 2014.

[5] "Coinbase - Your Hosted Bitcoin Wallet". *Coinbase*. Retrieved 30 November 2015.

[6] Fowler, Geoffrey A. (2014-02-18). "Bitcoin experiment in everyday life". *The Wall Street Journal*. Retrieved 2014-02-25.

[7] Fung, Brian. "Expedia wants you to book your next hotel stay with Bitcoin". The Washington Post. Retrieved 1 July 2014.

[8] Ember, Sydney (2014-09-10). "Coinbase Extends Bitcoin Access to International Customers". *The New York Times*. Retrieved 10 October 2014.

[9] "Dish Network Says It Will Accept Bitcoin". The New York Times. Retrieved 1 July 2014.

[10] Ludwig, Sean (2013-02-08). "Y Combinator-backed Coinbase now selling over $1M Bitcoins per month".

[11] Sarah E. Needleman (2013-05-07). "Coinbase Nabs $5M in Biggest Funding for Bitcoin Startup". *The Wall Street Journal*. Retrieved 10 October 2014.

[12] Alex Williams (2013-12-12). "Coinbase Raises $25M Led By Andreessen Horowitz To Build Its Bitcoin Wallet And Merchant Services". *TechCrunch*. Retrieved 2013-12-13.

[13] Cutler, Kim-Mai (2014-05-06). "Coinbase Acquires YC-Backed Kippt To Beef Up Its Product, Design Talent".

[14] Cutler, Kim-Mai (2014-08-18). "Coinbase Acquires Blockchain Explorer Blockr.io".

[15] Knight, Shawn (2014-09-01). "Coinbase has been insuring Bitcoin deposits for nearly a year".

[16] Burns, Matt (2013-12-21). "Overstock.com partners with Coinbase and starts accepting bitcoins as payment". *TechCrunch*. Retrieved 2014-01-10.

[17] Kharif, Olga. "Expedia to Accept Bitcoins for Online Hotel Bookings". *Bloomberg*. Retrieved 28 September 2014.

[18] "Expedia.com Now Accepts Bitcoin to Give Travelers More Choice and Flexibility in Hotel Payments". *Bloomberg*. Jun 11, 2014. Retrieved 28 September 2014.

[19] Rizzo, Pete. "Time Inc Becomes First Major Magazine Publisher to Accept Bitcoin". *Coindesk*. Retrieved 16 December 2014.

[20] Wilhelm, Alex (2014-07-18). "Dell Now Accepts Bitcoin For All Online U.S. Purchases". *TechCrunch*. Retrieved 2014-07-24.

[21] Del Rey, Jason (2014-03-27). "Stripe Merchants Will Soon Be Able to Accept Bitcoin Payments".

[22] Vigna, Paul; Casey, Michael (2015-01-20). "Coinbase raises 75 million in funding round". Wall Street Journal.

[23] Bensinger, Greg (2015-01-25). "First U.S. Bitcoin Exchange Set to Open". Wall Street Journal.

[24] "Coinbase to Shutdown CAD Services to Canadian Customers - CCN: Financial Bitcoin & Cryptocurrency News". *cryptocoinsnews.com*. 8 July 2016. Retrieved 23 July 2016.

[25] "Top 100 Blockchain Organisations: From CoinDesk to BitPay, These Are the Most Influential Organisations in the Distributed Ledger Space". *Richtopia*. Retrieved 21 May 2016.

[26] "Blockchain Organisations Top 100". *Blockchain Age*. Retrieved 3 June 2016.

[27] Shin, Laura (20160520). "Digital Currencies Show Potential To Be New Asset Class As Demand For Bitcoin Rival Ethereum Rises". *forbes.com*. Retrieved 23 July 2016. Check date values in: |date= (help)

[28] Tepper, Fitz (2016-07-21). "Coinbase is adding support for Ethereum". *techcrunch.com*. Retrieved 23 July 2016.

[29] Reisinger, Don (2014-09-11). "Bitcoin platform Coinbase expands to 13 European countries".

[30] "Coinbase Exchange Documentation". 2015-01-26.

5.8 Huobi

Huobi (⍰⍰⍰) is a Chinese digital currency trading platform and exchange based in Beijing.[1][2][3][4][5][6]

It was founded in September 2013.

It is one of the largest digital currency exchanges in China.[7]

5.8.1 References

[1] "Chinese Bitcoin Exchange Huobi 'Loses 5,000 BTC' in £1.2m Blunder". *International Business Times UK*.

[2] "Huobi Launches USD Exchange With 24/7 Customer Support". *CoinDesk*.

[3] "Huobi's BitVC Takes Trader Profit to Cover $1 Million Loss". *CoinDesk*.

[4] "Huobi Will Now Take Your Bitcoins as Stock Trading Collateral". *CoinDesk*.

[5] "After Crackdown, a New Bitcoin King Emerges in China". *WIRED*. 9 January 2014.

[6] "Pando: Huobi's new fixed-interest bitcoin investment product should have the hairs on your neck standing at attention". *Pando*.

[7] "Huobi emerges as leading bitcoin platform in China". *wantchinatimes.com*.

5.9 ItBit

itBit is a financial services company that offers a suite of bitcoin trading services, including a global bitcoin exchange and over-the-counter (OTC) trading desk. The company launched in November 2013.

In May 2015, itBit received a trust charter [1] from the New York State Department of Financial Services (DFS) and became the first company to operate a regulated bitcoin exchange in the United States.

itBit received more than US$5 million in venture capital [2] from Canaan Partners, RRE Ventures, Liberty City Ventures, and angel investors Jay W. Jordan II and Ben Davenport in their initial funding round. itBit's Series A round raised $25 million from RRE Ventures, Liberty City Ventures and others.

The company is headquartered in New York with an international office in Singapore.

5.9.1 References

[1] Bitcoin Exchange itBit Gets N.Y. Trust Charter, Bank Partner

[2] itBit Debuts Bitcoin Currency Exchange

5.10 LocalBitcoins

LocalBitcoins is a bitcoin startup company based in Helsinki, Finland. Its service facilitates over-the-counter trading of local currency for bitcoins.[2] Users post advertisements on the website, where they state exchange rates and payment methods for buying or selling bitcoins. Other users reply to these advertisements and agree to meet the person to buy bitcoins with cash[3] or pay with online banking. LocalBitcoins also offers a reputation and feedback mechanism for users and an escrow and conflict-resolution service. As of December 2013, LocalBitcoins has around 110,000 active traders with a trade volume of 1400–3000 bitcoins per day.[4]

In February 2014, two Florida men were charged with violating state money laundering laws for using LocalBitcoins.com.[5] In that same month the company announced that it would begin mass-producing low-cost bitcoin ATMs.[6] April 2016, another two men from Louisiana, a former Shreveport chiropractor and his son plead guilty to funneling money through an unlawful Bitcoin financial scheme. The men were using localbitcoins to advertise their services.[7]

5.10.1 References

[1] "LocalBitcoins | CrunchBase Profile". Crunchbase.com. Retrieved 2014-02-19.

[2] McMillan, Robert (2013-03-28). "Why the Only Real Way to Buy Bitcoins Is on the Streets | Wired Enterprise". Wired.com. Retrieved 2014-02-19.

[3] Murphy, Kate (July 31, 2013). "Virtual Currency Gains Ground in Actual World". New York Times. Retrieved February 20, 2014.

[4] Lemarchand, Rafael (2013-12-06). "Helsinki's LocalBitcoins Hits Up To €3 Million A Day In Exchanges". Arcticstartup.com. Retrieved 2014-02-19.

[5] "LocalBitcoins.com Targeted". Business Insider. 2014-02-09. Retrieved 2014-02-19.

[6] Joon Ian Wong (2014-02-15). "LocalBitcoins Starts Manufacturing Low-Cost Bitcoin ATM". Coindesk.com. Retrieved 2014-02-19.

[7] Elliot Maras (2016-05-23). "Arrests And Prosecutions Reveal Big Vagaries In Bitcoin Selling Regulations". cryptocoinsnews.com. Retrieved 2016-05-23.

5.10.2 External links

- Official website

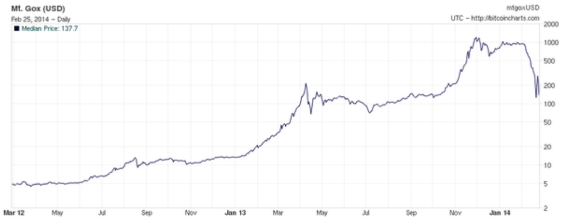
5.11 Mt. Gox

Mt. Gox was a bitcoin exchange based in Tokyo, Japan. It was launched in July 2010, and by 2013 was handling 70% of all bitcoin transactions.[1] In February 2014, the Mt. Gox company suspended trading, closed its website and exchange service, and filed for a form of bankruptcy protection from creditors called *minji saisei*, or civil rehabilitation, to allow courts to seek a buyer.[2][3] In April 2014, the company began liquidation proceedings.[4] It announced that around 850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $450 million at the time.[5][6] Although 200,000 bitcoins have since been "found", the reason(s) for the disappearance—theft, fraud, mismanagement, or a combination of these—were initially unclear. New evidence presented in April 2015 by WizSec lead them to conclude that "most or all of the missing bitcoins were stolen straight out of the MtGox hot wallet over time, beginning in late 2011."[7]

5.11.1 Founding

In late 2006, programmer Jed McCaleb (eDonkey2000, Overnet1, Ripple, Stellar) thought of building a website for users of the *Magic: The Gathering Online* service to let them trade cards like stocks.[8] In January 2007, he purchased the domain name mtgox.com, short for "Magic: The Gathering Online eXchange".[9][10][11][12] Initially in beta release,[13] sometime around late 2007, the service went live for around 3 months before McCaleb moved on to other projects, having decided it was not worth his time. He reused the domain name in 2009 to advertise his card game *The Far Wilds*.[14]

In July 2010, McCaleb read about bitcoin on Slashdot,[15] and decided that the bitcoin community needed an exchange for trading bitcoin and regular currencies after writing an exchange website, he launched it while reusing the spare mtgox.com domain name.[8]



Logarithmic scaled bitcoin price history in USD on the Mt. Gox exchange from February 2012 until its shutdown in February 2014

> I created mtgox on a lark after reading about bitcoins last summer. It has been interesting and fun to do. I'm still very confident that bitcoins have a bright future. But to really make mtgox what it has the potential to be would require more time than I have right now. So I've decided to pass the torch to someone better able to take the site to the next level.

5.11.2 2011

On 19 June 2011, a security breach of the Mt. Gox bitcoin exchange caused the nominal price of a bitcoin to fraudulently drop to one cent on the Mt. Gox exchange, after a hacker allegedly used credentials from a Mt. Gox auditor's compromised computer illegally to transfer a large number of bitcoins to himself. He used the exchange's software to sell them all nominally, creating a massive "ask" order at any price. Within minutes the price corrected to its correct user-traded value.[16][17][18][19][20][21] Accounts with the equivalent of more than $8,750,000 were affected.[18] In order to prove that Mt.Gox still had control of the coins, the move of 424,242 bitcoins from "cold storage" to a Mt.Gox address was announced beforehand and executed in Block 132749.[22]

In October 2011, about two dozen transactions appeared in the block chain (Block 150951)[23] that sent a total of 2,609 BTC to invalid addresses. As no private key could ever be assigned to them, these bitcoins were effectively lost. While the standard client would check for such an error and reject the transactions, nodes on the network would not, exposing a weakness in the protocol.

5.11.3 2013

On 22 February 2013, following an introduction of new anti-money laundering requirements by Dwolla, some Dwolla accounts became temporarily restricted. As a result, transactions from Mt. Gox to those accounts were cancelled by Dwolla. The funds never made it back to Mt. Gox accounts. Mt. Gox help desk issued the following comment: "Please be advised that you are actually not allowed to cancel any withdrawals received from Mt. Gox as we have never had this case before and we are working with Dwolla to locate your returned funds." The funds were finally returned on May 3, more than 3 months later, with a note "Please be advised never to cancel any Dwolla withdrawals from us again".

In March 2013, the bitcoin transaction log or "blockchain" temporarily forked into two independent logs with differing rules on how transactions could be accepted. The Mt. Gox bitcoin exchange briefly halted bitcoin deposits. Bitcoin prices briefly dipped by 23% to $37 as the event occurred[24][25] before recovering to their previous level in the following hours, a price of approximately $48.[26]

By April 2013 the site had grown to handle 70% of the world's bitcoin trades.[27] With prices increasing rapidly, Mt. Gox suspended trading from 11–12 April for a "market cooldown".[28] The value of a single bitcoin fell to a low of $55.59 after the resumption of trading before stabilizing above $100. Around mid May 2013, Mt. Gox traded 150,000 bitcoins per day, per Bitcoin Charts.[29]

On 2 May 2013 CoinLab filed a $75 million lawsuit against Mt. Gox alleging a breach of contract.[30] The companies had formed a partnership in February 2013 under which CoinLab handled all of Mt. Gox's North American services.[30] CoinLab's lawsuit contends that Mt. Gox failed to allow them to move existing U.S. and Canadian customers from Mt. Gox to CoinLab.[30]

On 15 May 2013 the US Department of Homeland Security (DHS) issued a warrant to seize money from Mt. Gox's US subsidiary's account with payment processor Dwolla.[31] The warrant suggests the US Immigration and Customs Enforcement, an investigative branch of the DHS, felt that the subsidiary, which was not licensed by the US Financial Crimes Enforcement Network (FinCEN), was operating as an unregistered money transmitter in the US.[31][32] Between May and July more than $5 million were seized.[29] On 29 June 2013, Mt. Gox received its money services business (MSB) license from FinCEN.[32]

On August 5, 2013, Mt. Gox announced that they incurred "significant losses" due to crediting deposits which had not fully cleared and that new deposits would no longer be credited until the funds transfer was fully completed.[33]

5.11.4 Insolvency and shutdown

Mt. Gox suspended withdrawals in US dollars on June 20, 2013.[34] The Mizuho Bank branch in Tokyo that handled Mt. Gox transactions pressured Mt. Gox from then on to close its account.[29] On July 4, 2013, Mt. Gox announced that it had "fully resumed" withdrawals, but as of September 5, 2013, few US dollar withdrawals had been successfully completed.[35][36][37]

Wired Magazine reported in November 2013 that customers were experiencing delays of weeks to months in withdrawing funds from their accounts.[27] The article said that the company had "effectively been frozen out of the U.S. banking system because of its regulatory problems". Customer complaints about long delays were mounting as of February 2014, with more than 3300 posts in a thread about the topic on the Bitcoin Talk online forum.[38]

On 7 February 2014, all bitcoin withdrawals were halted by Mt. Gox.[39] The company said it was pausing withdrawal requests "to obtain a clear technical view of the currency processes".[39] The company issued a press release on February 10, 2014 stating that the issue was due to transaction malleability: “A bug in the bitcoin software makes it possible for someone to use the bitcoin network to alter transaction details to make it seem like a sending of bitcoins to a bitcoin wallet did not occur when in fact it did occur. Since the transaction appears as if it has not proceeded correctly, the bitcoins may be resent. MtGox is working with the bitcoin core development team and others to mitigate this issue.”[40][41]

On 17 February 2014, with all Mt. Gox withdrawals still halted and competing exchanges back in full operation, the company published another press release indicating the steps they claim they are taking to address security issues.[42] In an email interview with the *Wall Street Journal*, CEO Mark Karpelès refused to comment on increasing concerns among customers about the financial status of the exchange, did not give a definite date on which withdrawals would be resumed, and wrote that the exchange would impose “new daily and monthly limits” on withdrawals if and when they were resumed.[43] A poll of 3000 Mt. Gox customers by CoinDesk indicated that 68% of customers were still awaiting funds from Mt. Gox. The median waiting time was between one and three months. 21% of poll respondents had been waiting for three months or more.[44]

On 20 February 2014, with all withdrawals still halted, Mt. Gox issued yet another statement, giving no date for the resumption of withdrawals.[45] A protest by two bitcoin enthusiasts outside the building that houses the Mt. Gox headquarters in Tokyo continued. Citing “security concerns”, Mt. Gox announced they had moved their offices to a different location in Shibuya. Bitcoin prices quoted by Mt. Gox dropped below 20% of the prices on other exchanges, reflecting the market’s estimate of the unlikelihood of Mt. Gox paying their customers.[46][47]

On 23 February 2014, Mark Karpelès, the CEO of Mt. Gox, resigned from the board of the Bitcoin Foundation.[48] The same day, all posts on their Twitter account were removed.[49]

On 24 February 2014, Mt. Gox suspended all trading, and hours later its website went offline, returning a blank page.[50][51][52] An alleged leaked internal crisis management document claimed that the company was insolvent, after losing 744,408 bitcoins in a theft which went undetected for years.[50][51][53][54] Six other major bitcoin exchanges released a joint statement distancing themselves from Mt. Gox, shortly before Mt. Gox’s website went offline.[55][56]

On 25 February 2014, Mt. Gox reported on its website that a “decision was taken to close all transactions for the time being”, citing “recent news reports and the potential repercussions on MtGox’s operations”. The chief executive, Mark Karpelès, told *Reuters* that Mt. Gox was “at a turning point”.[57][58][59][60]

In a January 6, 2015 interview[61] Kraken CEO Jesse Powell discussed being appointed by the bankruptcy trustee[62] to assist processing claims.[63]

5.11.5 Legal action

On 28 February 2014 Mt. Gox filed for bankruptcy protection in Tokyo, reporting that it had liabilities of about 6.5 billion yen ($64 million at the time), and 3.84 billion yen in assets.[64][65] The company said they had lost almost 750,000 of its customers’ bitcoins, and around 100,000 of its own bitcoins, totaling around 7% of all bitcoins, and worth around $473 million near the time of the filing.[64][65] Mt. Gox released a statement saying “The company believes there is a high possibility that the bitcoins were stolen,”[6] blaming hackers,[29] thus beginning a search for the missing money. The Chief Executive of Mt. Gox, Mark Karpelès, said technical issues opened up the way for fraudulent withdrawals.

Mt. Gox also faces lawsuits from its customers.[66][67]

On 9 March 2014, Mt. Gox filed for bankruptcy protection in the US, to temporarily halt U.S. legal action by traders who alleged the operation was a fraud.[68][69][70]

On 20 March 2014, Mt. Gox reported on its website that it found some bitcoins — worth around $116 million — in an old digital wallet from 2011. That brings the total number of bitcoins the firm lost down to 650,000 from 850,000.[71]

On April 14, Mt. Gox lawyers said that Mark Karpeles would not appear for a deposition in a Dallas court, or heed a subpoena by FinCEN.[29] On 16 April 2014, Mt. Gox gave up its plan to rebuild under bankruptcy protection, and asked a Tokyo court to allow it to be liquidated.[72]

5.11.6 See also

- Digital currency exchanger

5.11.7 References

[1] Vigna, Paul (2014-02-25). “5 things about Mt. Gox’s crisis”. *The Wall Street Journal*.

[2] McLannahan, Ben (2014-02-28). “Bitcoin exchange Mt Gox files for bankruptcy protection”. *Financial Times*.

[3] Abrams, Rachel; Goldstein, Matthew; Tabuchi, Hiroko (2014-02-28). “Erosion of Faith Was Death Knell for Mt. Gox”. *The New York Times*.

[4]

[5] Abrams, Rachel; Popper, Nathaniel (2014-02-25). “Trading Site Failure Stirs Ire and Hope for Bitcoin”. *The New York Times*.

[6] Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss, Carter Dougherty and Grace Huang, Bloomberg News, Feb. 28, 2014

[7] Nilsson, Kim (19 April 2015). “The missing MtGox bitcoins”. Retrieved 10 December 2015. Most or all of the missing bitcoins were stolen straight out of the MtGox hot wallet over time, beginning in late 2011

[8] Statement by McCaleb February 2014

[9] “Mt. Gox’s Original Creator Is At Work On A Secret Bitcoin Project”. *TechCrunch*. AOL. Retrieved 24 February 2015.

[10] “5 Things About Mt. Gox’s Crisis”. *WSJ*. Retrieved 24 February 2015.

[11] “Stripe Backs Non-Profit Decentralized Payment Network Stellar, From Mt. Gox’s Original Creator”. *TechCrunch*. AOL. Retrieved 28 April 2015.

[12] “Mt. Gox bitcoin exchange closure could help legitimize the currency.”. *Slate Magazine*. Retrieved 24 February 2015.

[13] “Internet Archive Wayback Machine”. Retrieved 24 February 2015.

[14] “The Far Wilds: Free Online Strategy Game”. Archived from the original on 12 August 2009. Retrieved 24 February 2015.

[15] http://ripple.com/blog/interview-with-jed-mccaleb-inventor-of-the-ripple-protocol-and-cofounder-of-opencoin/

[16] Karpeles, Mark (30 June 2011). “Clarification of Mt Gox Compromised Accounts and Major Bitcoin Sell-Off” (Press release). Tibanne Co. Ltd. Archived from the original on 19 September 2014.

[17] *Bitcoin Report Volume 8 - (FLASHCRASH)*. YouTube BitcoinChannel. 19 June 2011.

[18] Mick, Jason (19 June 2011). “Inside the Mega-Hack of Bitcoin: the Full Story”. *DailyTech*.

[19] Lee, Timothy B. (19 June 2011). “Bitcoin prices plummet on hacked exchange”. *Ars Technica*. Condé Nast.

[20] Mark Karpeles, 20 June 2011, Huge Bitcoin sell off due to a compromised account – rollback, Mt. Gox Support

[21] Chirgwin, Richard (19 June 2011). “Bitcoin collapses on malicious trade – Mt Gox scrambling to raise the Titanic”. *The Register*.

[22] “Block 132749 - Bitcoin Block Explorer”. Retrieved 24 February 2015.

[23] “Block 150951 - Bitcoin Block Explorer”. Retrieved 24 February 2015.

[24] Lee, Timothy. “Major glitch in Bitcoin network sparks sell-off; price temporarily falls 23%". *Ars Technica*. Condé Nast. Retrieved 12 March 2013.

[25] Blagdon, Jeff. “Technical problems cause Bitcoin to plummet from record high, Mt. Gox suspends deposits”. *The Verge*. Retrieved 12 March 2013.

[26] “Bitcoin Charts”. *Bitcoin Charts*.

[27] McMillan, Robert; Metz, Cade (6 November 2013). “The rise and fall of the world’s largest Bitcoin exchange”. *Wired*. Condé Nast. Retrieved 8 February 2014.

[28] “Twitter / MtGox: Trading is suspended until”. Twitter.com. Archived from the original on November 13, 2013. Retrieved 2014-02-17.

[29] Mochizuki, Takashi (20 April 2014). “Tracing a Bitcoin’s Exchange’s Fall From the Top to Shutdown Mark Karpelès hoped to set up a bitcoin cafe in the building where his exchange rented space.”. *WSJ*. Retrieved 22 April 2014.

[30] Chen, Adrian (2 May 2013). “Massive Bitcoin Business Partnership Devolves Into $75 Million Lawsuit”. *Gawker Media*. Retrieved 8 June 2013.

[31] Dillet, Romain (16 May 2013). “Feds Seize Assets From Mt. Gox’s Dwolla Account, Accuse It Of Violating Money Transfer Regulations”. *TechCrunch*. AOL Inc. Retrieved 10 February 2014.

[32] Buterin, Vitalik (29 June 2013). “MtGox Gets FinCEN MSB License”. *Bitcoin Magazine*. Coin Publishing Ltd. Retrieved 10 February 2014.

[33] “August 2013 Mt. Gox Status Update” (Press release). Mt. Gox Co. Ltd. 5 August 2013. Archived from the original on 5 August 2013.

[34] McMillan, Robert (20 June 2013). “Bitcoin’s Big Bank Problem: Why Did Mt. Gox Halt U.S. Payouts?". *Wired*. Condé Nast.

[35] Vigna, Paul (5 July 2013). “Bitcoin operator Mt. Gox resumes withdrawals”. *The Wall Street Journal*.

[36] Vigna, Paul (31 July 2013). “Bitcoin exchange Mt. Gox still grappling with slowdown”. *The Wall Street Journal*.

[37] Marron, Donald (3 September 2013). “How Bitcoin spreads violate a fundamental economic law”. *Forbes*.

[38] Wong, Joon Ian (4 February 2014). “Poll: Are you having Mt. Gox withdrawal issues?". *CoinDesk*. Retrieved 9 February 2014.

[39] Dougherty, Carter (7 February 2014). “Bitcoin Price Plunges as Mt. Gox Exchange Halts Activity”. *Bloomberg*. Retrieved 9 February 2014.

[40] “Update - Statement Regarding BTC Withdrawal Delays” (Press release). Mt. Gox Co. Ltd. 10 February 2014. Archived from the original on 10 February 2014.

[41] “mt gox shutdown puts bitcoin investors on edge - pokerupdate.com”. *pokerupdate.com*. Retrieved 24 February 2015.

[42] “20140217-Announcement: Tokyo, Japan, February 17th, 2014” (Press release). Tokyo: Mt. Gox. 17 February 2014. Archived from the original (PDF) on 17 February 2014. |archive-url= is malformed: timestamp (help)

[43] Mochizuki, Takashi & Warnock, Eleanor (February 17, 2014). “Bitcoin Platform Mt. Gox Apologizes for Delayed Response - CEO Karpeles Declines To Shed Light On How Customer Funds Are Protected”. Wall Street Journal.

[44] Wong, Joon Ian (15 February 2014). “68% of Mt. Gox Users Still Awaiting Their Funds, Survey Reveals”. Coin Desk.

[45] Clinch, Matt (February 20, 2014). “Bitcoin investor fury at Mt Gox delays”. CNBC.

[46] Byford, Sam (February 20, 2014). “Mt. Gox, where is our money?". The Verge.

[47] “Bitcoin exchange in Downward Spiral: “Mt Gox has left the building"". Hannover, Germany: Heise. February 20, 2014.

[48] “Mt. Gox resigns from Bitcoin Foundation”. *Reuters*. February 23, 2014. Retrieved 25 February 2014.

[49] “MtGox Resigns From Bitcoin Foundation, Deletes All Tweets From Twitter Feed”. Business Insider. February 23, 2014. Retrieved 25 February 2014.

[50] McMillan, Robert (24 February 2014). “Bitcoin exchange Mt. Gox implodes amid allegations of $350 million hack”. *Wired*. Retrieved 25 February 2014.

[51] Popper, Nathaniel; Abrams, Rachel (25 February 2014). “Apparent theft at Mt. Gox shakes Bitcoin world”. *The New York Times*. Retrieved 25 February 2014.

[52] Nagano, Yuriko; Wright, Stephen (25 February 2014). “Website of Bitcoin exchange Mt. Gox offline”. *Associated Press*. Retrieved 25 February 2014.

[53] How a bug in bitcoin led to MtGox’s collapse, Alex Hern, The Guardian, Feb. 27, 2014

[54] Kathryn Glass. “Internet Chat Reveals Mt. Gox CEO Hasn't 'Given Up'". *Fox Business*. Retrieved 24 February 2015.

[55] “Bitcoin exchange Mt. Gox’s website down”. *Reuters*. 25 February 2014. Retrieved 25 February 2014.

[56] “The Coinbase Blog - Joint Statement Regarding MtGox”. *The Coinbase Blog* (Press release). Coinbase. 24 February 2014. Retrieved 24 February 2014.

[57] “Mt. Gox website says all transactions closed “for the time being"". *Reuters*. 25 February 2014. Retrieved 25 February 2014.

[58] Lowery, Adrian (25 February 2014). “Is it the beginning of the end for Bitcoin? Virtual currency in turmoil as rumoured $375m theft closes major exchange”. *This is money*. Retrieved 25 February 2014.

[59] Anklam, Fred (25 February 2014). “Bitcoin exchange Mt. Gox goes offline amid turmoil”. *USA Today*. Retrieved 25 February 2014.

[60] Vaishampayan, Saumya (25 February 2014). “Mt. Gox says transactions closed 'for time being'". *Market Watch*. Retrieved 25 February 2014.

[61] “Interview with Jesse Powell,” Bitcoin Knowledge Podcast, January 6, 2015.

[62] Powell, Jesse. “MtGox Bankruptcy Trustee”. *We Use Coins*. Retrieved 6 January 2015.

[63] “Kraken Accepting MtGox Bankruptcy Claims and Giving Free Trade Credit”. *Bitcoin Magazine* (Press release). Bitcoin Magazine. 22 April 2015. Retrieved 12 May 2015.

[64] Warnock, Eleanor; Mochizuki, Takashi; Martin, Alexander (28 February 2014). “Mt. Gox files for bankruptcy protection”. *The Wall Street Journal*. Retrieved 28 February 2014.

[65] Takemoto, Yoshifumi; Knight, Sophie (28 February 2014). “Mt. Gox files for bankruptcy, blames hackers for losses”. *Reuters*. Retrieved 28 February 2014.

[66] Sidel, Robin (28 February 2014). “Almost Half a Billion Worth of Bitcoins Vanish”. *Wall Street Journal*. Retrieved 3 March 2014.

[67] “MtGox Boss Sued For Bitcoin Losses”. *Investing.com*. 4 March 2014.

[68] Finley, Klint (10 March 2014). “Bitcoin Exchange Mt. Gox Files for U.S. Bankruptcy as Death Spiral Continues”. *Wired*. Retrieved 11 March 2014.

[69] Hals, Tom (10 March 2014). “Mt. Gox files U.S. bankruptcy, opponents call it a ruse”. *Reuters*. Retrieved 11 March 2014.

[70] “Bitcoin exchange Mt. Gox files for US bankruptcy”. *New York Post*. 10 March 2014. Retrieved 11 March 2014.

[71] Karpeles, Mark (2014-03-20). "⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰ / Announcement regarding the balance of Bitcoin held by the company” (PDF). MtGox. Retrieved 2014-03-22. MtGox Co., Ltd. had certain oldformat wallets which were used in the past and which, MtGox thought, no longer held any bitcoins. Following the application for commencement of a civil rehabilitation proceeding, these wallets were rescanned and their balance researched. On March 7, 2014, MtGox Co., Ltd. confirmed that an oldformat wallet which was used prior to June 2011 held a balance of approximately 200,000 BTC (199,999.99 BTC).

[72] Takashi MochizukiAnd Katy Stech (16 April 2014). “Mt. Gox Files for Liquidation”. *WSJ*. Retrieved 24 February 2015.

5.11.8 External links

- Official website
- MtGox Co., Ltd. bankruptcy docket from the United States Courts Archive

5.12 OKCoin

OKCoin is the largest Bitcoin company in China with core product lines of a Bitcoin exchange, and a mobile consumer payment and lending app. OKCoin operates the largest Bitcoin exchange and through blockchain technology, seeks to dramatically improve payment systems. OKCoin Exchange China operates CNY/BTC spot pair with margin trading from its Beijing entity, while OKCoin International operates USD/BTC spot pair with margin trading and BTC/USD futures from its Singapore entity.

As of August 2016, OKCoin is the largest Bitcoin exchange in the world with a volume of over 16,000,000 Bitcoins per month.[1]

5.12.1 History

OKCoin was founded by CEO Star Xu in 2013 and has raised US$10mm in investments from Ceyuan Ventures, Mantra Capital, Ventures Lab and other notable private investors including Silicon Valley investor Tim Draper.

Star Xu is an experienced technology executive.Professionally, Star worked at Yahoo/Alibaba as a search algorithm engineer before serving as Chief Technical Officer of DocIn.com – a popular file sharing company – where he managed a team of 120 engineers.[2]

OKCoin has publicly expressed intention to expand overseas and become a worldwide digital currency services company.[3]

5.12.2 Controversy

On May 23, 2015, OKCoin made public a contractual dispute the company was having with Roger Ver over the management rights to the domain name “bitcoin.com.”[4] OKCoin management claimed that they could no longer pay Ver the money which was contractually owed to him due to a recent case in which Ripple Labs was fined $700,000 by FinCEN for failure to collect proper KYC paperwork from Ver.[5] In response, Ver published several months of email history between himself and OKCoin demonstrating that OKCoin had not been making payments for several months prior to the news about Ripple’s fine.[6] In the emails, OKCoin CEO Star Xu claims to have discovered a more recent version of the contract signed by both parties, which included a clause that gave OKCoin the right to terminate the contract upon six months notice. Until this point, all communications between the two parties had been cryptographically signed using GPG, but Ver was able to prove that the newer version of the contract was signed with the same timestamped signature he appended to the previous version of the contract, indicating that his signature was merely copied over to the new document.[7] OKCoin proceeded to make a public offer of a $20,000 reward for anyone who was able to prove that Ver’s statements were false; Ver responded in kind by offering a $1,000,000 reward to anyone who could prove that the signature on the more recent contract was actually valid and not a forgery.[7] The OKCoin reward was paid at the end of May, 2015 following the report of analysis of the contracts posted publicly by OKCoin.[8]

5.12.3 References

[1] “Bitcoin Charts / Markets”. *www.bitcoincharts.com*. Retrieved 2016-08-06.

[2] “The China King of Bitcoin: Star Xu - BEIJING, June 10, 2014 /PRNewswire/". Prnewswire.com. Retrieved 2014-06-30.

[3] Jon Southurst (@southtopia) (2014-05-19). “OKCoin and Huobi Discuss Bitcoin in China and Plans for Survival”. Coindesk.com. Retrieved 2014-06-30.

[4] OKCoin) (2015-05-23). “OKCoin no longer managing Bitcoin.com due to contract conflict with domain owner”. OKCoin Blog. Retrieved 2015-05-26.

[5] Stan Higgins) (2015-05-05). “FinCEN Fines Ripple Labs for Bank Secrecy Act Violations”. Coindesk. Retrieved 2015-05-26.

[6] Joseph Young) (2015-05-25). “Roger Ver and OKCoin Squabble over Bitcoin.com, Breach of Contract”. CoinTelegraph. Retrieved 2015-05-26.

[7] Allen Scott) (2015-05-25). “Roger Ver: 'I Will Offer a $1,000,000 Bounty to Anyone Who Can Prove I Signed that Contract'". CoinTelegraph. Retrieved 2015-05-26.

[8] Ben McGinnes (2015-05-29). “Analysis of OKCoin Documents”. Retrieved 2016-09-05.

5.12.4 External links

- http://www.forexminute.com/bitcoin/okcoin-inc-launches-algorithmic-trading-tools-on-its-trading-platfor
- http://www.prnewswire.com/news-releases/the-china-king-of-bitcoin-star-xu-262529321.html

Chapter 6

Text and image sources, contributors, and licenses

6.1 Text

- **Bitcoin** *Source:* https://en.wikipedia.org/wiki/Bitcoin?oldid=741071066 *Contributors:* Damian Yerrick, Eloquence, Zundark, The Anome, Tommy~enwiki, Roybadami, Edward, Canton, Nealmcb, Michael Hardy, Fred Bauder, Liftarn, Ixfd64, Cyde, TakuyaMurata, DavidWBrooks, Kingturtle, Julesd, Pratyeka, Glenn, Ciphergoth, Theamer, Mike Linksvayer, Susurrus, Grin, Samw, Ed Brey, Dcoetzee, Fuzheado, Andrewman327, WhisperToMe, Tpbradbury, Furrykef, Cleduc, Shizhao, Topbanana, Dbabbitt, AnonMoos, Drernie, Jni, Lambda, Nurg, Pjedicke, Rfc1394, Markewilliams, DataSurfer, Pifactorial, Tea2min, David Gerard, Psb777, DavidCary, Nelson Minar, Gil Dawson, Fudoreaper, HangingCurve, MSGJ, Marcika, Gus Polly, Dratman, Gamaliel, Micru, Jorge Stolfi, Gracefool, Daniel Brockman, Wiki Wikardo, Esrogs, Isidore, Utcursch, Pgan002, R. fiend, SarekOfVulcan, OverlordQ, Quarl, IGEL, Kaldari, Oneiros, DragonflySixty-seven, Bosmon, Bodnotbod, Mayosmith, Kevin143, Byset, Shadypalm88, Thorwald, T-Boy, SYSS Mouse, Shiftchange, AliveFreeHappy, Rudd-O, Robert Horning, Discospinster, Brianhe, Rich Farmbrough, Tere, Pmsyyz, Zombiejesus, Smyth, Cagliost, D-Notice, Arthur Holland, TimBray, Gronky, Bender235, Mike Hearn, Jgarzik, Neko-chan, Pjf, Kwamikagami, Emeitner, Mr. Strong Bad, Art LaPella, Tgeller, PatrikR, BalanceUT, Cretog8, Aceat64, Truthflux, Stesmo, Billymac00, Smalljim, Beachy, John Vandenberg, C S, Makomk, Giraffedata, Palmcluster, 99of9, BenM, Mattl, Officiallyover, Gary, Terrycojones, MrTree, Bnicklin, The RedBurn, Mizerydearia, Vaelor, Graingert, Jonathanriley, Theodore Kloba, Spangineer, Atomicthumbs, Teggles, Wtmitchell, Velella, Rebroad, Quintin3265, Runtime, Tony Sidaway, Geraldshields11, DaveInAustin, Dzhim, Dduane, Drbreznjev, Recury, Voxadam, Martian, Hyfen, Dismas, Daranz, Zntrip, Feezo, AustinZ, Bobrayner, Gmaxwell, Dandv, ApLundell, Shadeofblue, Danmaz74, MattGiuca, Pol098, Tabletop, GregorB, Mattmorgan, Stcalvert, Fleetham, BD2412, Qwertyus, David Levy, Zzedar, Jclemens, Ses4j, Koavf, Isaac Rabinovitch, Jake Wartenberg, Hulagutten, Helvetius, Strait, XP1, ColdWind, Mikesc86, Jrn0074, Ekspiulo, Ttwaring, Syced, Diablo-D3, SystemBuilder, Ground Zero, Akihabara, KarlFrei, Ysangkok, Crazycomputers, Intgr, Lmatt, Sperxios, OpenToppedBus, Schandi, Mrschimpf, Alec.brady, Benlisquare, 020543m, Voodoom, Bgwhite, Manscher, Fcs, Aalegado, Wavelength, ThunderPeel2001, Conchisness, Mrienstra, Huw Powell, Cyferx, MJustice, Red Slash, Chosenken, Bhny, Pi Delport, Hydrargyrum, Stephenb, Sneak, David Woodward, Danuthaiduc, NawlinWiki, Teb728, GSK, E123, Arichnad, P The D, Joel7687, Harksaw, Vivaldi, FML, Tony1, Zythe, Deku-shrub, Luke-Jr, Morgan Leigh, Eclipsed, Black Falcon, MarkBrooks, Unforgiven24, Ott2, Genjix, Cmskog, Ripper234, LarryLACa, Johndrinkwater, Pyronite, Ninly, Nikkimaria, Arthur Rubin, Bondegezou, Modify, Netrapt, Richardbondi, Petri Krohn, Pifvyubjwm, Paulsnx2, Shawnc, Back ache, Katieh5584, Merlinthe, Tom Morris, Chronosilence, SmackBot, Ashenai, Kosik, C.Fred, Ginot, Elwood j blues, KVDP, Delldot, Crazyanimal, Wanders~enwiki, Rōnin, Timotheus Canens, Wittylama, Mauls, Tim@, SmartGuy Old, Yamaguchi⍰⍰, Gilliam, Portillo, Emj, Ohnoitsjamie, TrollDeBatalla, Sparge, Wcoenen, Chris the speller, Advorak, Thumperward, Elatanatari, GeraldKaszuba, V4vijayakumar, James Fryer, SvGeloven, Mdwh, Deli nk, Jerome Charles Potts, Jfsamper, Jdthood, Tekhnofiend, Kmag~enwiki, Ladislav Mecir, Lenin and McCarthy, Mike hayes, Famspear, Tamfang, Smallbones, Metallurgist, Frap, Zootreeves, Jtbobwaysf, Rrburke, Xyzzyplugh, Kittybrewster, WhereAmI, Blue Matt, Fiskbullar, Ddas, Speedplane, WaldoJ, RolandR, BackDraft9387, Derek R Bullamore, Clean Copy, Nonstopdrivel, Sokolesq, Webjoe, Meni Rosenfeld, Piedmont, Springnuts, Juneblender, Byelf2007, Paul 012, Lambiam, Mike the k, Dmh~enwiki, Kaputa12, John, ZAB, Robofish, Plaiche, IronGargoyle, Nagle, Tymothy, Melody Concerto, Makyen, Davemcarlson, Larrymcp, Meco, Dr.K., AdjustablePliers, Jcmorin, Dl2000, Jimisdead, Pjrm, Norm mit, DouglasCalvert, Iridescent, Kencf0618, Jmchugh, Clarityfiend, Courcelles, WakiMiko, TiriPon, Mikeyfaces, FatalError, Geremia, Jackzhp, Risoto2000~enwiki, Matthieu Houriet, Mgumn, The Cake is a Lie, JohnCD, Jokes Free4Me, N2e, Penbat, Thepm, Cydebot, Cahk, Danrok, Snarpel, ChristTrekker, Reywas92, Steel, Gogo Dodo, Jedonnelley, Maged123, Bposert, DumbBOT, Hontogaichiban, Biblbroks, Kozuch, Sckirklan, Arb, PamD, Ishdarian, Headbomb, Parsiferon, Davidhorman, EdJohnston, Gnurkel, Floridasand, Kjj31337, Izyt, Mmortal03, Utopiah, KrakatoaKatie, Ileresolu, CLSwiki, Seaphoto, Lovibond, Activist, Smartse, Mack2, Jdhowlett, Kmcnamee, JonathanCross, Ingolfson, Steelpillow, Daytona2, Deadbeef, Leuko, Dereckson, Barek, MER-C, Skomorokh, Sonicsuns, Bidofthis, OhanaUnited, Andonic, Dscotese, Mwarren us, Gert7, Magioladitis, Swikid, Firenu, Yakushima, JamesBWatson, SHCarter, Nyttend, Froid, Destynova, I JethroBT, JLMadrigal, Tekn04, Sipa1024, Logictheo, Mjbauer, Craig Mayhew, JaGa, TimidGuy, Gwern, Oren0, FisherQueen, Ekki01, Jimmilu, Rsraleigh, CommonsDelinker, Xiphosurus, ShoWPiece, Metallaxis, Trusilver, Maurice Carbonaro, Headinthedoor, Manderso, Smite-Meister, Maproom, Toobaz, Lordgilman, 10mbt, Laytonsmith14, Tarinth, Leonarbe, NewEnglandYankee, Ontarioboy, Yablochko, Misbach, Tyraz, Ultra two, KylieTastic, Corriebertus, Ross Fraser, Ajfweb, Bonadea, Scott Illini, Pdcook, BernardZ, Loopback007, Davidr89, Cuzkatzimhut, VolkovBot, Thomas.W, Rubyuser, Fences and windows, Dom Kaos, Toddy1, QuackGuru, Redpointist, Philip Trueman, Oshwah, Giszmo~enwiki, Jogar2, Burpen, Sbjf, Chuckwolber, HannahKon, JUBAL-CAIN, Someguy1221, Cloudswrest, Jakebed, Rjm at sleepers, Noformation, Atheros1, UnitedStatesian, Unknownlight, Sheridan Zhoy, Ale85, Larklight, Agyle, Billinghurst, PeterEasthope, Cooperh, Poltair, Celosia, Tigerchen, Ecnirpnaf99, Jakub Vrána, Groceryheist, TheLastNinja, Jehorn, Ellomate, DestroyerofDreams, EverGreg, Ponyo, TJRC, Swliv, Hertz1888, OldCar, Znmeb, Gatopeich, X-Fi6, Yintan, Revent, Araignee, Soler97, Gts 2000, Bentogoa, Flyer22 Reborn, Jimthing, EditorInTheRye, Rodarmor, SPACKlick, Jonahtrainer, DMNT, SimonTrew, Int21h, Oniscoid, Cépey, Metalsmyth, Svick, Stfg, S2000magician, HighInBC, Randomblue, MarkMLl, Tradereddy, Mr. Stradivarius, Dabomb87, Denisarona, VanishedUser sdu9aya9fs787sads, ImageRemovalBot, Mr. Granger, Sfan00 IMG, Verbaetlittera, Elassint, Keyur mithawala, SummerWithMorons, Jbening, Ethridgela, Dmurashchik, Blueyed, Cambrasa, KeithyIrwin, Quinxorin, Drmies, Der Golem, Frmorrison, Leopard850, SuperHamster, Niceguyedc, Kamillas 1, Jswd, LeoFrank, Kitsunegami, Excirial, Socrates2008, Watchduck, Karlhendrikse, Sebleouf, NathanWalther, DrCroco, Arjayay, Tuchomator, Snacks, Tony Holkham, JasonAQuest, NintendoFan, Ecureuil espagnol, Chrisarnesen, Zootboy, SF007, Lironah, M.qrius, Twofivethreetwo, Jtjathomps, XLinkBot, Laser brain, Dthomsen8, Mitch Ames, Galzigler, CapnZapp, Beach drifter, Mrcatzilla, MystBot, Jabberwoch, Glavkos, Dbrisinda, Addbot, Mckinley99, Mortense, Grayfell, FrankAndProust, Antonio92~enwiki, Thomasee73, AlbinoFerret, Mike30188, Mootros, TutterMouse, Frankensite, IceCreamEmpress, PhilosophyKing, Download, LaaknorBot, JasonCooney, Neilonidas, NittyG, Favonian, Rook944, Jasper Deng, AgadaUrbanit, 84user, Ehrenkater, Equilibrium007, Josh Keen, Cesiumfrog, Jarble, Mutorq, Сергей Олегович, Softy, The Bushranger, Ben Ben, Legobot, Acmilan15, Luckas-bot, Zhitelew, Yobot, Fraggle81, Louisstar, Legobot II, Ddcorkum, Amirobot, Sobi3ch, Denispir, Aoxfordca, R2D2!, Edoe, Rick Raubenheimer, Torsch, GamerPro64, Jerebin, Kirov Airship, Masharabinovich, Vroo, Dickdock, 4th-otaku, Dmarquard, DavidHarkness, AnomieBOT, KDS4444, Wikiyakapoola, DemocraticLuntz, John Holmes II, Message From Xenu, Jim1138, Interligator, Keithbob, L3lackEyedAngels, Mann jess, Materialscientist, Are you ready for IPv6?, Citation bot, Object404, V8skittles, GB fan, ArthurBot, Teilolondon, LilHelpa, Xqbot, Huangpo, JimVC3, El33th4x0r, Crookesmoor, Aussiejohn, Mononomic, GenQuest, TheCuriousGnome, DataWraith, Gidoca, Dâniel Fraga, Jamescart, Srich32977, Mr.choppers, Sithishade, Solphusion~enwiki, Frettsy, Bizso, Omnipaedista, Orbixx, The Interior, Carrite, West Coast Gordo, KennethHan, RCraig09, Polargeo, Rasos, Sainibindass, A. di M., ASOTMKX, Sandro kensan, GliderMaven, Anna Roy, תומר א., Riventree, Hobsonlane, Mu Mind, Quinn d, UncleNinja, Sanpitch, WikiDonn, Alarics, Ptrinh18, RoyGoldsmith, Timos m, Haeinous, Mfwitten, Kenfyre, Marcel van b, Redcert, Alex.ryazantsev, Greggydude, Weirdo10o4, OgreBot, Redrose64, Dusanson, Extramaster, OriumX, Gautier lebon, Pinethicket, I dream of horses, Elockid, Alphazeta33, Lesath, Sanderd17, Intrepid-NY, Raphaelbastide, Calmer Waters, Smithd98, The.megapode, Hisabness, Henriwatson, ContinueWithCaution, Cathy Richards, Rholme, Kylebk, Niri.M, Kgrad, Soundcomm, Tbuckley89, Trappist the monk, Dchestnykh, Sirius-n, The Frenchie, Jesus Presley, Shelbymoore3, Throwaway85, Lotje, Krassotkin, Callanecc, Krisives, Athaba, Ponmudivn, Miracle Pen, Bluefist, Mattmill30, Mcharnay, Aoidh, Cowlibob, David Hedlund, Jadair10, No One of Consequence, Diannaa, Vanzandtj, Ivanvector, Fblan001, Chronulator, Skakkle, Stanjourdan, Suffusion of Yellow, EyeKnows, Skmacksler, Civic Cat, Jfmantis, Mean as custard, JjusticeIV, Dree12, RjwilmsiBot, Sargdub, Ripchip Bot, VernoWhitney, Vivek.m1234, Phlegat, Mchcopl, Opticbit, HeinzzzderMannn, Kiko4564, Rollins83, Steve03Mills, Rayman60, EmausBot, Cricobr, WikitanvirBot, Rathergood15, Observer6, Nuujinn, Philippe (WMF), Mjdtjm, Jibbsisme, Dewritech, GoingBatty, RA0808, Marco Guzman, Jr, Gardaud, Gogophergo, Antiquax, Qrsdogg, Klbrain, Torturella, NorthernKnightNo1, Your Lord and Master, Steve Lux, Jr., Mmeijeri, Wikipelli, Dcirovic, Gagarine, Kaskaad, K6ka, Zeallous, Werieth, JDDJS, Grondilu, ZéroBot, QuentinUK, John Cline, Checkingfax, Josve05a, Bollyjeff, Humanist09, Melksoft, Érico, Leotheleo, Mrmatiko, Eugene4444, Jonpatterns, Fortheloveofbacon, Yiosie2356, 7partparadigm, SporkBot, Arpabone, L0ngpar1sh, Ocaasi, Casascius, Andre.Koster, Coubs514, JoeSperrazza, Gonzo.Lubitsch, Libertaar, 0Core0, CJDuhaime, Palosirkka, Spobin, Gsarwa, Donner60, SBaker43, Do3cc~enwiki, Bulwersator, Ipsign, ChuispastonBot, Gandrewstone, AndyTheGrump, JanetteDoe, Targaryen, Jav wiki, Elph, Kai445, Ebehn, Doc Merlin, TitaniumCarbide, Davey2010, Voomoo, Cgt, Petrb, Mikhail Ryazanov, ClueBot NG, HLachman, Johnnyshocker, Gareth Griffith-Jones, George strawberry, Ulflund, Somedifferentstuff, Verpies, Ypnypn, LogX, Gilderien, Satellizer, Exposo, Polargeo 3, Tcatm, Magic1million, Vacation9, Loginnigol, Kjrreid, Mahir256, Bussings, Imperi, YuMaNuMa, Korrawit, Matt06012011, Seancasey00, OverQuantum, Bazuz, Tabletrack, Mathew105601, ParkKimLim, Frietjes, Dreth, Porkloinson, Luziusmeisser, Asukite, VinceSamios, Cyborg4, Widr, Heyandy889, Nicboman, Newyorkadam, Ryan Vesey, Lawsonstu, Barry McGuiness, Slushcz, Gerritharkness, Oddbodz, Helpful Pixie Bot, MS10EL, Ericsheldon, Rhydic, Cojovo, Aesir.le, Calabe1992, Guest2625, Hostfat, Emisanle, Jeraphine Gryphon, Technical 13, Da5id403, Leandro.cesar, Lowercase sigmabot, BG19bot, Justintbassett, Roberticus, Dvtimes99, Esoteric10, FuFoFuEd, Astrohacker, Criticcon, WikiTryHardDieHard, The editor1900, Iselilja, Werowe, 13Goldem, Dpacmittal, Jcnetsys, Proudnewly1, Maccollie, Brustopher, ThereNHere, Batouzo, Neøn, ThisIsNotReal, McZusatz, JesseT77, Global Standard, MusikAnimal, Ecurrencies, Nikos 1993, Bitcoineer, Cavirtex, GKFX, Sharpseek, Elucches, WinampLlama, Mark Arsten, Vermillion trade, Miraje182, Fbarousse, BitcoinTomWilliams, Socialmaven1, Exercisephys, Falkirks, Dmoores55, Juggernauts10, ChrisPDX, Izmailov, Mascarponette, FormerNukeSubmariner, Terry4forex, Ainderbyquernhow, Ivan.a.tikhonov, Peterowenwilson, Majorbolz, Crh23, Bob Re-born, TheMacMini09, U4ealongan, Lxndr, MrBill3, GoCubs88, Rivoton, Victorsharpe, Tesssla, Cliff12345, Thegreatgrabber, Klilidiplomus, TheGoodBadWorst, Steve.alleny, Rutebega, Cleanelephant, Clearish, Hamez0, Winston Chuen-Shih Yang, Samwalton9, MeanMotherJr, BattyBot, Factsearch, Sonba, Tkbx, Tutelary, Mleeds12, David.moreno72, ~riley, Testem, Zhaofeng Li, Kabesang Tales, JayBeeCool, Swctg, Cyberbot II, Phelix77, 0x0F, ChrisGualtieri, Larmsterpoet, JimNelin, CrunchySkies, Iolaka91823972, Electricmuffin11, Polarandwet, Earl King Jr., Khazar2, Momposi, Xoviat, MSUGRA, MohammedBinAbdullah, Tow, DJFission, OsmanRF34, Jockzain, Rezonansowy, TobyGoodwin, Swenkman, Codename Lisa, Black Rainbow 999, Mogism, Citation Needed, Guss82, Kbog, Kephir, Doggum, Cerabot~enwiki, TippyGoomba, Lone boatman, Farmenergybars, Bitenthusiast, Lutworth, MrAndreessen, Nonnompow, Lugia2453, Hto9950, Leptus Froggi, Frosty, Osyed1, Statecraft, HowardStrong, ComfyKem, Andyhowlett, 123sage321, Ezzayakoo, SPECIFICO, W1k1p3d1a26, Danny Sprinkle, Gowthamkare, Telfordbuck, Leijurv, Another John S, Mariagvozd, BurritoBazooka, Gatenosix, BeachComber1972, Anonymous68th, PinkAmpersand, Sr.ganador, Epicgenius, SolarStarSpire, Tsgesq, BitBus, Hotelmason241, Ianpurton, Ruby Murray, Play Money for Dummies, Tomato expert1, Neoconfederate, EricLarson80, Mbmexpress, Kap 7, Surfer43, Dairhead, TinkleBear, Alfy32, Wuerzele, Tango303, Dvdlevy120, RaphaelQS, JacquelineDerrida, Thkie, Flat Out, Byung do jung, New worl, Sarath divakar, Suumitgeek, KyleLandas, Akh81, Ndeine, NorthBySouthBaranof, FischTank, NYC.Geek, Klakurka, 51coin, Patrick2409, NottNott, MisterHungry, JoshDieter, Someone not using his real name, JeanLucMargot, Sam Sailor, Keepinternetfree, Jianhui67, Archlinux, TCMemoire, Oumot, MrScorch6200, DarkestElephant, DPRoberts534, XTC99LLC, Bojo1498, CameraWallet, Pinetreecrush, LaFayettePolitico, Lemonsdrops, Fixuture, Crow, JaconaFrere, G S Palmer, Lakun.patra, Marc Bago, Eliteware, JexsterB312, Tunacanoe, Unicodesnowman, ExtremeHeat11, CogitoErgoSum14, Vcwatcher, Mikhat, CarnivorousBunny, Encrypto1, Yoshi24517, Nyashinski, Jaumenuez, YubbaDoo, Craigrottman, Currency cobano, Mattpalen, Silbtsc, Mojargon, BitcoinWiki, Hypnopompus, XDexus, Pigpie45, Bitbain, Krautsk, Wiki man 195, Concord hioz, Monkbot, BarnstarFactory, BerkeleyLaw1979, JorgeGabriel, Powerful Lomax, Volker Siegel, Teaksmitty, Litecoinguy, Kitsios.a, J.vayner, SantiLak, OKNoah, Seppelpeters, Abckhxkcvrtyu, Zulfikar ramzan, Wikifanman33, Dsprc, TitmanTrolled, BkDJk, Blue oracl2495, Manishvyas1747, Rextexesq, QuantOfAsia, Ali78v, Bobby223322, Shotsmc, Hats2543, Shadowzdx, ChrNPal, Qwertym77, Mollyjohn1436, BitcoinrealityCheck, TwoEscarf, 12uihy, PirdPirdPrid, Milidepe, Paulpocket, LampWithALeaf, WwATuu, Urunak, MARIODOESBREAKFAST, FOXIBOX, LoseKabel, Hannasnow, Robert-Rhys, Henryb2000, 10pippe, Bitslots, ChocTinFoil, LeeParq, Chunchi8, Hitechcomputergeek, Vilalna, Titfditroyl, Superdavywavy, Eliteness, SpiltOctacle, MonteDaCunca, Unframboise, Thegrubbsian, Imthewinner, Vinnie james, DissidentAggressor, Rooley555, Immanuel Thoughtmaker, UneCanardNoire, Myfare, HMSLavender, Ozzke, BitMeistern, Julia Eremina, Anotherusername1, Coin Collecting John, Zowayix001, Vwm3nelson, Homni, Wasill37, HamishPassion, Mozzzus, Akemaschite, Mario Castelán Castro, Caliburn, Phrackage, TheMagikCow, Kshanti07, Randomuser0122, ChamithN, Expresscoin, Bastian crypto, Webdesignersnow, AydinC, Tmarie3753, Jack Matelot, Jsthack, BITPUMP, Mtahaalam, BondNewYork, Adeyaya, Sysuwxm, Sealyy, TBroe, Primealgorith, Creationlayer, Liance, ThePenultimateOne, Brianrisk, Tenaqzn'f Fbvyrq Gubat, Wuerzele2, E3b0c, Donate Bticoin, Rog31905, TheCoffeeAddict, YossiBoroPark, Esquivalience, Weegeerunner, Buchanjim, Marksel, 4455tyui, Lothlorien317, BitTony, Vatadoshu, BoA-BTCopsec-14, TyHeers, Craftdraw, Sizeofint, SoSivr, GimmeOpenRoad, Nysrtup, Acruxlilt, THE GREY LINER, Kraainem, SaffronBacchus, BashCo, DiogoCão, Jimmylone, SpiryGolden, Ster3oPro, MariaAnnaWien, Zahirfahmi, I enjoy sandwiches, MLODROB, KasparBot, Ceannlann gorm, Samalter, Rickshawcraw, Pharoah237, BitcoinX, LJWiki2000, Brollymook, 666AngelOfDeath, DylanMcKaneWiki, ʬ, Pyrros, Contentry, Milko Zec, Wywyit, Pendletonian, VirtuOZ, Cashregister225, Malibubarbie, PeterVanDerStraaten, BU Rob13, NorwayStorm, Gaelan, Furious Mythical Beast, D4m13nb3rry, FiddleFudger, Chevvin, PetitMonsieur, Thereisnous, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Dr Lotus Black, FOSBusters, Pocketapocketa, Sftty, Cockblower, Brandonb01, AdmiredSneeze, 1FVLiNNTM65cxZ1rErevtEBLGHxzDMnVRY, Bitcoin Guy, Weltenstuermer, Qzd, Scott085, Ecoinseo, KryptoNatasha, 30has09, Mdclxvi0, Ghost of hugh glass, Игорь Олегович 20.11., Jeffboh, Dertyqwerty, Oreigdor, Optimised, Btcvia, Chrimas1, BearGlyph, Johnwk, AppMaster1000, AtErik1, PointedToTheMoon, Earl King and Anonymous: 969

- **History of Bitcoin** *Source:* https://en.wikipedia.org/wiki/History_of_bitcoin?oldid=741339045 *Contributors:* AxelBoldt, Fnielsen, Edward, Dj ansi, David Latapie, Dbabbitt, Chealer, Gil Dawson, Gracefool, Mormegil, Nwerneck, Stesmo, David Levy, Rjwilmsi, Akihabara, Ysangkok, Catsmeat, Benlisquare, Bgwhite, Red Slash, Hydrargyrum, Rsrikanth05, Luke-Jr, Puritan Nerd, Bondegezou, Rathfelder, Jerome Charles Potts, Ladislav Mecir, Frap, WhereAmI, MilborneOne, IronGargoyle, Kencf0618, Kozuch, Floridasand, JonathanCross, Xhienne, Nyttend, PStrait, Bonadea, Philip Trueman, Agyle, Jonahtrainer, Int21h, TheCatalyst31, Sfan00 IMG, Mild Bill Hiccup, UltraEdit, Chrisarnesen, Mhockey, Download, LuK3, Zhitelew, AnomieBOT, Netscr1be, Citation bot, Ywaz, Alumnum, Yefi, Geoffmenegay, Sanpitch, Breadblade, Jonesey95, David Hedlund, Rschnall, Dree12, RjwilmsiBot, John of Reading, Dewritech, GoingBatty, Dcirovic, Werieth, QuentinUK, Checkingfax, SporkBot, Palosirkka, AndyTheGrump, ClueBot NG, Onanoff, Frietjes, Chisme, VinceSamios, Cyborg4, BG19bot, IlCyborg, Cliff12345, Merrittttt, Josemanuelgp, Samwalton9, BattyBot, Cyberbot II, ChrisGualtieri, Khazar2, Rezonansowy, Mogism, Kbog, Ikesham, Adam2us, PC-XT, Mbmexpress, KyleLandas, Qetrix, NorthBySouthBaranof, Someone not using his real name, Marcila28, Gracesfall, SamanthaPuckettIndo, Impsswoon, JexsterB312, Thegentlemanfromtralfamadore, Unicodesnowman, Pythonideus, Mercury's Stepson, Olenyash, BarnstarFactory, Rextexesq, Gsync, Lolpootis, FlyBEET, Hannasnow, MonteDaCunca, Den82~enwiki, Adeyaya, Chrisbarnes67, SoSivr, Stepbang, ʬ, Srednuas Lenoroc, Pendletonian, Websoftwarerev, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Mbevand, Pictomania and Anonymous: 71

- **Legality of bitcoin by country** *Source:* https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country?oldid=738913585 *Contributors:* Tommy~enwiki, Roadrunner, Roybadami, Jorge Stolfi, PatrikR, Stesmo, Apokrif, Fleetham, Akihabara, Benlisquare, Bgwhite, Rsrikanth05, Eclipsed, Josh3580, Yamaguchi□□, Ladislav Mecir, Cemeraslan, Meni Rosenfeld, Nagle, Runderwo, VanHelsing.16, Gafter, Cydebot, Kozuch, Floridasand, Repku, Monkeyjunky, Ontarioboy, Agyle, Kellypeters, Hotbelgo, Unbuttered Parsnip, Michele.mostarda, Arjayay, Chrisarnesen, Mhockey, Mitch Ames, Mrcatzilla, Grayfell, Download, Josh Keen, Zhitelew, Yobot, Bearas, AnomieBOT, Materialscientist, Pipeafcr, Jeune17, Haripetrov, Lady Lotus, Jonesey95, Cerevisae, Arbero, Trappist the monk, Lotje, David Hedlund, Herun1988, Dree12, Misconceptions2, John of Reading, MrFawwaz, Dewritech, Checkingfax, Derekleungtszhei, AManWithNoPlan, CJDuhaime, GermanJoe, Iketsi, ClueBot NG, Joefromrandb, Mahir256, Hahahafr, VinceSamios, BG19bot, WikiTryHardDieHard, Riyantojayadi, BattyBot, David.moreno72, ArmorShieldA99, Enterprisey, Rezonansowy, Mogism, Vengadora, Surfer43, Soffredo, Wuerzele, DavidLeighEllis, Mareksip, CyrusV, Habarithor, SamanthaPuckettIndo, Unicodesnowman, Mattpalen, Silbtsc, Monkbot, CV99, GinAndChronically, Ks91020, 10pippe, BitMeistern, Huuku, Jelly Bean MD, Homni, Wasill37, Phrackage, Jonoweltman, EoRdE6, Esquivalience, Matshenricson, Ictgeek, Pzez, Goenkas, Juan José García Chávez, Srednuas Lenoroc, Bitcoinina, Saintv2, Tiseko88, Gautam Shetty, Qzd, Cumisfun, Chalitshee and Anonymous: 67

- **Satoshi Nakamoto** *Source:* https://en.wikipedia.org/wiki/Satoshi_Nakamoto?oldid=740782038 *Contributors:* Enchanter, Mrwojo, Michael Hardy, Kaihsu, David Latapie, Fuzheado, Greenrd, Jeffq, Huangdi, Bearcat, Auric, JackofOz, Mdmcginn, Ævar Arnfjörð Bjarmason, Wiki Wikardo, Thorwald, Zombiejesus, Smyth, TerraFrost, Mike Hearn, Glenn Willen, Etnoy, John Vandenberg, Deryck Chan, Gargaj, GregorB, Tlroche, Koavf, Vegaswikian, Ysangkok, Crazycomputers, Catsmeat, Czar, Intgr, Lmatt, Wester, Stan2525, Bhny, Matt Fitzpatrick, Hydrargyrum, Anomalocaris, Korny O'Near, Dissolve, Abune, CharlesHBennett, SmackBot, McGeddon, Mauls, Gilliam, Ladislav Mecir, Racklever, Icerat, Jtbobwaysf, Soap, Ben Moore, BillFlis, Kothog, Yugyug, CalebNoble, Jesse Viviano, Penbat, Staberinde, Widefox, Obiwankenobi, Yellowdesk, JonathanCross, FuriouslySerene, Magioladitis, TGGP, Oren0, Anaxial, ChrisfromHouston, Maproom, Katharineamy, Misbach, Sigmundur, Ajfweb, Black Kite, Mercurywoodrose, Agyle, Y, BrianRecchia, Jkalltheway, OldCar, Flyer22 Reborn, Lagrange613, Randomblue, Niceguyedc, NuclearWarfare, TheRedPenOfDoom, SF007, Karpouzi, Mortense, FrankAndProust, 84user, OlEnglish, Jarble, Yobot, Carleas, Dmarquard, AnomieBOT, Materialscientist, G6cid, Gumok, Veryhappychappy, Omnipaedista, Patchy1, Rotideypoc41352, Sanpitch, Mistakefinder, Rhalah, Vicenarian, LittleWink, Woodcutterty, Aoidh, Yunesj, Tbhotch, Onel5969, Brkt, GoingBatty, Peaceray, Your Lord and Master, Dcirovic, Chihaya Sta, DuNnoxd, AvicBot, Checkingfax, Donner60, AndyTheGrump, ClueBot NG, □□□□□, Polargeo 3, Hahahafr, Newyorkadam, Guest2625, Emisanle, Aoidh (Away), BG19bot, KateWishing, WalterKin, Kendall-K1, David.karpay, Samwalton9, BattyBot, Codeh, Rezonansowy, Another John S, Bitcoin, Hopkinsenior, Rmehtany, Neoconfederate, Jodosma, Surfer43, Blythwood, Bahooka, Comp.arch, KyleLandas, NorthBySouthBaranof, Matrix142, TheycallmetheDoctor, Stamptrader, Thatonewikiguy, SamanthaPuckettIndo, Unicodesnowman, YubbaDoo, Henry Castor dos Santos, Felderburg, BusinessRules, Taco Viva, Flippzz, Augusto192, Hannasnow, KDDLB, CamelCase, Ywecur, KH-1, Handpolk, Satoshinakamotosan, Adeyaya, Creationlayer, Hollth, Danmabraham, Govindaharihari, Grocko1, Craftdraw, Roselyn Hamilton, Sss04, Kripmo, GeneralizationsAreBad, AlshMoudy, KasparBot, UrfinJ, Aduggan1234, Juhishadan, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Senoranandmanikutty, RoyalMer, Gulumeemee, Kayminmb, DougMaher, Roost btc, Anam 786 and Anonymous: 153

- **Hal Finney (cypherpunk)** *Source:* https://en.wikipedia.org/wiki/Hal_Finney_(computer_scientist)?oldid=726408775 *Contributors:* Mike Linksvayer, Rosarino, Bender235, Mjackson, Wikiklrsc, ArtDent, SmackBot, Sadads, Bradenripple, Robofish, Cydebot, Obiwankenobi, Connormah, Bongwarrior, Waacstats, Thibbs, Gwern, Ontarioboy, Ruukasu2005, Natg 19, DFRussia, Atepomaros, Chrisarnesen, Yobot, AnomieBOT, Unbitwise, RjwilmsiBot, Adits90, Catlemur, Wgolf, BG19bot, ArmorShieldA99, Cyberbot II, Clevera, Wuerzele, YubbaDoo, Creationlayer, KasparBot, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, RobbieIanMorrison and Anonymous: 17

- **Gavin Andresen** *Source:* https://en.wikipedia.org/wiki/Gavin_Andresen?oldid=722910218 *Contributors:* Lquilter, Samw, Bearcat, PulpSpy, YUL89YYZ, Koavf, Ysangkok, Back ache, Hmains, Jtbobwaysf, Derek R Bullamore, Timtrent, Cydebot, Obiwankenobi, DGG, R'n'B, Adavidb, Seudo, Aboutmovies, UnitedStatesian, Gbawden, Repat, Chrisarnesen, Tassedethe, Jerebin, AnomieBOT, Pmokeefe, Jadair10, Justinba1010, VinceSamios, BG19bot, Kendall-K1, Mark Arsten, Cliff12345, Plimptiplom, Wuerzele, YubbaDoo, Creationlayer, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 12

- **Nick Szabo** *Source:* https://en.wikipedia.org/wiki/Nick_Szabo?oldid=735962065 *Contributors:* Mike Linksvayer, Fuzheado, Phil Boswell, Xoloz, P The D, Mattythewhite, N2e, Penbat, Medovina, Obiwankenobi, Waacstats, Ontarioboy, Lamro, Chrisarnesen, Yobot, AnomieBOT, Sanpitch, Tom.Reding, Beyond My Ken, BG19bot, Daveman16, ChrisGualtieri, TortoiseWrath, Jodosma, DavidLeighEllis, Mercury's Stepson, YubbaDoo, Augusto192, Ferenstein, Yousefak123, Handpolk, Creationlayer, KasparBot, Pendletonian, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Flo626 and Anonymous: 8

- **Winklevoss twins** *Source:* https://en.wikipedia.org/wiki/Winklevoss_twins?oldid=738806347 *Contributors:* AnonMoos, Jerzy, Xanzzibar, Discospinster, Night Gyr, Lauciusa, Art LaPella, Dgpop, BDD, Dandv, Benbest, Kmg90, Karam.Anthony.K, RichardWeiss, Rjwilmsi, Ground Zero, Bgwhite, RussBot, Arichnad, SmackBot, Portillo, Derek R Bullamore, Will Beback, CmdrObot, MC10, SchutteGod, Widefox, Obiwankenobi, Waacstats, Vanished user ty12kl89jq10, NatGertler, George415, Mufka, Wikimandia, Agyle, Raivenblade, MBD123, GorillaWarfare, All Hallow's Wraith, Niceguyedc, Auntof6, Arjayay, Chrisarnesen, Ost316, Download, Yobot, Fraggle81, Tiller54, McAnt, Lady Lotus, Serols, RjwilmsiBot, Aircorn, EmausBot, MikeyMouse10, Checkingfax, Shuipzv3, A930913, General Fiasco, Surajt88, Targaryen, ClueBot NG, FreebirdBiker, Yale2013, BattyBot, Sscsasrs, Fraulein451, Cheerioswithmilk, Jecm1990, Everymorning, Sayitclearly, Jules871, NottNott, Bmrg567, Potenttomato, Frenchballmansquid, AbeFrohman1977, YubbaDoo, TropicAces, Script8man, TheMagikCow, Kshanti07, BD2412bot, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 56
- **Mark Karpelès** *Source:* https://en.wikipedia.org/wiki/Mark_Karpel%C3%A8s?oldid=733738559 *Contributors:* Wjhonson, David Gerard, Piotrus, Smyth, Smalljim, Saga City, Fragglet, DAJF, Deku-shrub, Jerome Charles Potts, Lenin and McCarthy, MagicalTux, Tbc42, Jesse Viviano, Danrok, Obiwankenobi, Magioladitis, Waacstats, Ajfweb, Oshwah, Agyle, All Hallow's Wraith, Willhwl, Underwaterbuffalo, 84user, AnomieBOT, Jonesey95, Ecafyelims, Dewritech, GoingBatty, Josve05a, ClueBot NG, Catlemur, Chisme, BG19bot, Squirelewis, Jeremy112233, UNOwenNYC, Epicgenius, Taco Viva, Dontthrowaway, Markkarpeles, TheCockroach, KasparBot, ʬ, ⍰⍰⍰⍰, CAPTAIN RAJU, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 40
- **Bitcoin Foundation** *Source:* https://en.wikipedia.org/wiki/Bitcoin_Foundation?oldid=737154948 *Contributors:* The Anome, Jayjg, Smyth, MBisanz, Bgwhite, MSJapan, Tom Morris, Kamenev, Kendrick7, Robofish, Cydebot, DumbBOT, Mmortal03, Magioladitis, DGG, Agyle, Clivemacd, Chrisarnesen, AnomieBOT, Alvin Seville, Aoidh, Reaper Eternal, Tbhotch, Checkingfax, Guest2625, BG19bot, Exercisephys, Safehaven86, Cyberbot II, Dexbot, Rezonansowy, Another John S, Doyouevenlift84, Mrpsystem, PizzaAddict, Gdesmedt1, Bitkoof, Olenyash, JRFORSYTH, Bomberjacket5, Okinawa55, Terry Rchardson, Srednuas Lenoroc, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Spendulus and Anonymous: 10
- **Bitcoin network** *Source:* https://en.wikipedia.org/wiki/Bitcoin_network?oldid=733888135 *Contributors:* Canton, Collabi, Julesd, Closeapple, Neko-chan, Stesmo, Giraffedata, Graingert, Wtmitchell, Benlisquare, Wavelength, Pburka, Deku-shrub, Delldot, Chris the speller, Jprg1966, Ladislav Mecir, Solarix, ZAB, MeekMark, Smartse, Lfstevens, Xhienne, Wootery, Magioladitis, Oren0, Enderminh, Jdeacon, Jonahtrainer, Daviderenne, SuperHamster, JustinClarkCasey, Arjayay, Chrisarnesen, Mortense, Fgnievinski, Jarble, Yobot, AnomieBOT, Wiki.gcc, Argumzio, OgreBot, Divinity76, Dree12, Xiangfu, Observer6, Mmeijeri, Dcirovic, Werieth, QuentinUK, Checkingfax, Coffeeandcode, GermanJoe, Targaryen, Jack Greenmaven, Catlemur, Aandaleeb85, VinceSamios, BG19bot, Falkirks, Cliff12345, BattyBot, ChrisGualtieri, Earl King Jr., Tmfs10, Rezonansowy, Me, Myself, and I are Here, Epicgenius, Dairhead, Wuerzele, Suumitgeek, Comp.arch, KyleLandas, Dalukasio, Eliteware, Bloukingfisher, SyaWgnignahCehT, Kevin514, Mattpalen, Melcous, Litecoinguy, Deepbit, MARIODOESBREAKFAST, FOXIBOX, JDLade, Hannasnow, Ozzke, Charlie7705, Zowayix001, Adeyaya, Creationlayer, GimmeOpenRoad, Bitcoinwhoswho, Tomaskulich, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Pvaish, Jpkabin, DatGuy, AllBestFaith and Anonymous: 46
- **Cryptocurrency** *Source:* https://en.wikipedia.org/wiki/Cryptocurrency?oldid=740873653 *Contributors:* Canton, Greenman, IMSoP, David Latapie, Hyacinth, Dbabbitt, Chealer, Altenmann, David Gerard, Cool Hand Luke, Thomas Veil, Mormegil, Hydrox, Smyth, Closeapple, Stesmo, V2Blast, Hoary, Mindmatrix, Sburke, Benbest, Sjakkalle, Rjwilmsi, Equitor, DVdm, Volunteer Marek, Bgwhite, Bradtem, Dialectric, Deku-shrub, Eclipsed, Ripper234, DoriSmith, NeilN, Resolute, Melchoir, Darkstar1st, Kintetsubuffalo, Sektah, Ladislav Mecir, BlackTerror, AThing, A. Parrot, Kencf0618, Mikes1988, N2e, Penbat, Krauss, Guineapigs, DumbBOT, Sobreira, JustAGal, Barek, Maqayum, Albany NY, Extropian314, Magioladitis, Rdubeau, Froid, Smite-Meister, Riffraffselbow, Don4of4, Wiae, Agyle, Cindamuse, RMJJRM, RatnimSnave, Jonahtrainer, Roxor128, Markvtc, Elassint, Clivemacd, Gherson2, VQuakr, Doseiai2, Niceguyedc, Jreiss17, Another Believer, Chrisarnesen, Mjbauer95, Fgnievinski, Jncraton, MrOllie, Erik Streb, Eculewatt, Yobot, Jerebin, ONaNcle, AnomieBOT, Materialscientist, Eumolpo, Hromi, GliderMaven, FrescoBot, Ivoras, Hellknowz, Rditucci, Wimmeljan, AMuraliKumar, Mcharnay, Aoidh, Cowlibob, C4K3, Mean as custard, EmausBot, Tuankiet65, Lucien504, Super48paul, Dewritech, Ballofstring, Dcirovic, K6ka, John Cline, Checkingfax, Jonpatterns, I'm not human, JoeSperrazza, Wadaad, Sonicyouth86, Mikhail Ryazanov, ClueBot NG, Cpabon, Catlemur, Mahir256, Wdchk, Mathew105601, VinceSamios, Widr, Kevoras, Cojovo, Wbm1058, Emisanle, BG19bot, WikiTryHardDieHard, MusikAnimal, Mark Arsten, Amritamaz, Blaspie55, Vario, Cliff12345, FeralOink, BattyBot, Factsearch, Mleeds12, ArmorShieldA99, Mdann52, 0x0F, ChrisGualtieri, Rfkrishnan, Leostaley, IjonTichyIjonTichy, Enterprisey, Rezonansowy, Citation Needed, AldezD, Sidelight12, Chustuck, Sr.ganador, Randykitty, Alfredymora, Sudoquai, Neoconfederate, Surfer43, Dairhead, GRIFFnDOOR, Hendrick 99, Jakec, Soffredo, Wuerzele, DavidLeighEllis, Comp.arch, KyleLandas, Matuhin86, Stirling7, FDMS4, AnonymousWiking, RainCity471, Someone not using his real name, Ppcoinwikipeercoin, Grjgt893u34, Nerdcustoms, Djnickers, Alienwalkerx, Unicodesnowman, DiddlyDoes, StableCoin, Mikandjo, Mercury's Stepson, YubbaDoo, SemiSynthPsy, Bitsumishi, Permafrost46, Panos Skourtis, NataliWinehouse, Concord hioz, Monkbot, Towtol, Huey2323, Kumarovski, Davidbentolila, Aniapie, Coincq, Keycoin, Dsprc, Salsacz, Eristas, Spireanet, Beachdanny, DNotescoin, Catoshi, Paulpocket, RtrebWnordl, Bels11, Hannasnow, Croteaumj, Everettjustin, FursuitYiff, Pelecoin123456, Banjokid2000, Ozzke, Vwm3nelson, Mozzzus, Starroc, TheMagikCow, MitchellMint, Narky Blert, Sealyy, Rainbowtrail, WinterstormRage, ThePenultimateOne, Pishcal, TheCoffeeAddict, NielThiart, Stanley.garland, Arthistorian1977, Huckleberry15, SpiryGolden, Cryptowest, I enjoy sandwiches, Vindicated8912, CAPTAIN RAJU, Wikihelpful, BrokenCrypto, Raymon Johnstone, Dataronin, MaxKordek, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Agar.ioSUCKSBUTT, Hayleyithink, Calcorn7, Dylanpoor, DatGuy, Aximov, Asienbummler2, Cryptofanz, Cryptoedge and Anonymous: 176
- **Elliptic Curve Digital Signature Algorithm** *Source:* https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm?oldid=734627696 *Contributors:* Danny, Imran, Michael Hardy, Shellreef, CesarB, Cyp, Giftlite, Inkling, Matt Crypto, CryptoDerk, TonyW, ArnoldReinhold, Bender235, Barcex, Davidgothberg, Huerlisi, Kelly Martin, Mandarax, Maxal, Siddhant, Gene.arboit, Tony1, Arthur Rubin, KnightRider~enwiki, Rtc, GBL, Ekalin, LouScheffer, DRLB, TastyPoutine, Daniel5127, Cydebot, Synergy, Widefox, Dimawik, JAnDbot, Pbroks13, Pharaoh of the Wizards, Smite-Meister, Flyingstar16, Trosati, Bugbee, Phil Bridger, Annie Yousar, Leobold1, Duncan, FiloSottile, Addbot, Darhuuk, MrOllie, Yobot, MarioS, KamikazeBot, Zxb, Nageh, Winterst, Ale And Quail, Olawlor, Ripchip Bot, John of Reading, Arkenflame, Catlemur, Lundril, Chmarkine, ChrisGualtieri, Dexbot, SoledadKabocha, Namnatulco, Nonnompow, Mark viking, Dncsky, ThomasPopp, Claw of Slime, YubbaDoo, BkDJk, RGMoonen, Chrisseberino, Hackancuba and Anonymous: 54
- **Peer-to-peer** *Source:* https://en.wikipedia.org/wiki/Peer-to-peer?oldid=740136804 *Contributors:* Damian Yerrick, AxelBoldt, Kpjas, Wesley, The Anome, RoseParks, Rjstott, Andre Engels, Greg Lindahl, Youssefsan, Aldie, M~enwiki, SimonP, Ben-Zin~enwiki, Ellmist, Heron, Dk~enwiki, Branko, Olivier, Chuq, Jim McKeeth, Edward, Ubiquity, K.lee, Michael Hardy, Kwertii, Lexor, Lousyd, Shellreef,

Kku, Liftarn, Gabbe, Collabi, Delirium, Eric119, Minesweeper, CesarB, Mkweise, Ahoerstemeier, Copsewood, Haakon, Mac, Ronz, TUF-KAT, Yaronf, Kingturtle, Ping, LittleDan, Julesd, Pratyeka, Glenn, Sir Paul, Rossami, Rl, Jonik, Thebramp, Conti, Schneelocke, Mydogategodshat, Frieda, Timwi, MatrixFrog, Viajero, Wik, IceKarma, Rvalles, Maximus Rex, Sweety Rose, Furrykef, Itai, Bhuston, Meembo, SEWilco, Omegatron, Ed g2s, Bloodshedder, Dysfunktion, MadEwokHerd, Johnleemk, Jamesday, Owen, Chuunen Baka, Robbot, Paranoid, MrJones, Sander123, Korath, Tomchiukc, ZimZalaBim, Tim Ivorson, Postdlf, Texture, Yacht, TittoAssini, Qwm~enwiki, Mushroom, Anthony, Cyrius, Moehre, Jrash, RyanKoppelman, Rossgk, Connelly, Giftlite, DocWatson42, Fennec, DavidCary, Laudaka, ShaunMacPherson, Mintleaf~enwiki, Wolfkeeper, Netoholic, Lupin, Bkonrad, Niteowlneils, Endlessnameless, FrYGuY, Gracefool, AlistairMcMillan, Softssa, VampWillow, Benad, Jrdioko, Neilc, PeterC, Fys, Toytoy, Knutux, Lockeownzj00, Thomas Veil, ArneBab, Lord dut, Hgfernan, Secfan, Maximaximax, Vbs, Wiml, Korou, Ihsuss, Jareha, Lee1026, Cynical, Joyous!, Kevyn, DMG413, Ivo, The stuart, Shiftchange, Mormegil, Tom X. Tobin, DanielCD, Lifefeed, Discospinster, 4pq1injbok, Sharepro, Solitude, Rich Farmbrough, Rhobite, Iainscott, Till Ulen, H0riz0n, Jon Backenstose, Inkypaws, Jsnow, Morten Blaabjerg, Deelkar, Bender235, S.K., Loren36, Mjohnson, CanisRufus, Gen0cide, Koenige, Tverbeek, PhilHibbs, Diomidis Spinellis, Sietse Snel, Just zis Guy, you know?, Eltomzo, Grick, LBarsov, Velociped, BrokenSegue, Johnteslade, Unquietwiki, SpeedyGonsales, VBGFscJUn3, Minghong, Idleguy, Wrs1864, Haham hanuka, Merope, Conny, Ifny, Liao, Mo0, Falsifian, CyberSkull, Gwendal (usurped), Andrewpmk, Cctoide, Sl, Apoc2400, Antoniad, Gaurav1146, Elchupachipmunk, Snowolf, Eekoo, Melaen, Gbeeker, Totof, Raraoul, ReyBrujo, Stephan Leeds, Evil Monkey, Tony Sidaway, Computerjoe, Versageek, Gene Nygaard, Ringbang, Netkinetic, MiguelTremblay, Ceyockey, Adrian.benko, AlexMyltsev, Mahanga, Kelly Martin, Mindmatrix, Vorash, The Belgain, Jersyko, Morton.lin, Deeahbz, Splintax, Abab99, Ilario, Ruud Koot, The Wordsmith, MONGO, Mangojuice, Wtfunkymonkey, Rchamberlain, CharlesC, Waldir, Sendai2ci, Wayward, Toussaint, Karam.Anthony.K, Palica, Gerbrant, Aarghdvaark, Zephyrxero, David Levy, Kbdank71, Phoenix-forgotten, Canderson7, CortlandKlein, Sjakkalle, Kumarbhatia, Rjwilmsi, Quale, Strait, PinchasC, Tawker, Forage, Edggar, Kry~enwiki, Peter Tribe, LjL, Bhadani, -lulu-, FlaBot, Authalic, Ground Zero, RexNL, Ewlyahoocom, Mike Van Emmerik, Valermos, RobyWayne, Bmicomp, Chobot, Garas, Bgwhite, Manu3d, Dadu~enwiki, Cuahl, YurikBot, Wavelength, Borgx, Pip2andahalf, RussBot, Wellreadone, Akamad, Gaius Cornelius, CambridgeBayWeather, Bovineone, Salsb, Richard Allen, Msoos, Johann Wolfgang, Nick, Retired username, Mikeblas, RL0919, Amwebb, Matthewleslie, Nethgirb, Mavol, Wangi, DeadEyeArrow, Atbk, Bota47, Charleswiles, Xpclient, Nlu, Bikeborg, Boivie, FF2010, Zzuuzz, 2bar, Lt-wiki-bot, Ninly, Bayerischermann, Icedog, Closedmouth, Abune, GraemeL, Adammw, Fram, Scoutersig, Rearden9, Sunil Mohan, Bluezy, Carlosguitar, Maxamegalon2000, Teryx, GrinBot~enwiki, BiH, Aimini, Prab, Elbperle, Veinor, Zso~enwiki, SmackBot, Evansp, Xkoalax, Reedy, Unyoyega, Augest, Od Mishehu, Cutter, Vald, Bomac, Echoghost, Arny, KelleyCook, HalfShadow, Preeeemo, Yamaguchi⍰⍰, Gilliam, Ohnoitsjamie, Folajimi, Skizzik, Chris the speller, Bluebot, Coinchon, Jprg1966, Emufarmers, Thumperward, Victorgrigas, Carlconrad, Octahedron80, Trek00, DHN-bot~enwiki, Konstable, Audriusa, Royboycrashfan, Kzm, Mirshafie, Neiltheffernaniii, Милан Јелисавчић, Preada, TCL, Ultra-Loser, Nixeagle, JonHarder, Rrburke, Zak123321, Vironex, NoIdeaNick, Radagast83, E. Sn0 =31337=, Bslede, Jiddisch~enwiki, Funky Monkey, Bernino, Allyant, Jeremyb, Sigma 7, LeoNomis, Cjdkoh, Ck lostsword, Alcuin, Pilotguy, Kukini, Ricky@36, Mbauwens, P2pauthor, SashatoBot, Nishkid64, Harryboyles, Tazmaniacs, Rjdainty1, Gobonobo, Aaronchall, Joshua Andersen, InfinityB, Musicat, Generic69, Scyth3, Flamingblur, F15 sanitizing eagle, Loadmaster, Silvarbullet1, JHunterJ, Mauro Bieg, Tigrisnaga, Ryulong, Rosejn, Peyre, Caiaffa, Teemuk, Fan-1967, Iridescent, Michaelbusch, BrainMagMo, Sschluter, Sirius Wallace, Thommi, Az1568, Courcelles, Gounis, Pjbflynn, Tawkerbot2, FatalError, SkyWalker, JForget, CmdrObot, Bane004, Zarex, Miatatroll, Pmerson, GargoyleMT, Requestion, Pgr94, Kennyluck, Cldnails, Arangana, Phatom87, Ooskapenaar, Jackiechen01, ECELonghorn, Steel, Gogo Dodo, Feedloadr, Farshad83, Vanished user 8jq3ijalkdjhviewrie, DumbBOT, FastLizard4, Kozuch, Nuwewsco, Daniel Olsen, Lo2u, Gimmetrow, Thijs!bot, Epbr123, Coelacan, Oldiowl, Headbomb, Nick Number, Wikidenizen, AntiVandalBot, Lord JoNil, Ingjerdj, Bondolo, Caper13, Bigjimr, Leuko, Davewho2, Dustin gayler, CosineKitty, Albany NY, BrotherE, Geniac, SteveSims, Magioladitis, Antelan, Bongwarrior, VoABot II, Dekimasu, Yandman, JamesBWatson, CobaltBlue, Radio Dan, Mupet0000, Gabriel Kielland, Pausch, M 3bdelqader, 4nT0, Cpl Syx, Kgfleischmann, Deathmolor, RayBeckerman, Stephenchou0722, Aliendude5300, Sachdevj, MartinBot, LinuxPickle, Rettetast, Akkinenirajesh, Webpageone.co.uk, Mattsag, LedgendGamer, Tgeairn, Brunelstudy, Mthibault, Feierbach, Hopper96, Icseaturtles, Karrade, LordAnubisBOT, Touisiau, Wuyanhuiyishi, Aervanath, Cometstyles, SirJibby, Warlordwolf, Remember the dot, Ghacks, Lawman3516, Ahtih, Stanleyuroy, Idioma-bot, Funandtrvl, Soali, Jimmytharpe, VolkovBot, ABF, Hansix~enwiki, Jeff G., Indubitably, I'mDown, Philip Trueman, Smywee, Hpfreak26, TouristPhilosopher, Someguy1221, Coldfire82, Una Smith, Lradrama, LotharZ, Seb26, Jackfork, LeaveSleaves, Buryfc, Anishsane, Haseo9999, Gillyweed, SmileToday, VanishedUserABC, Hardistyar, Kbrose, Exile.mind, SieBot, Kwirky88, BotMultichill, Gerakibot, Caltas, Rexguo, Terribim, ACNS, Dattebayo321, Bentogoa, Flyer22 Reborn, Permacultura, Reinderien, Matthewedwards, Bagatelle, Cshear, Lightmouse, Hobartimus, Kos1337tt, Mattycl, Creative1980, DRTllbrg, Jludwig, Phelfe, Tomdobb, Stedjamulia, Celique, Tuxa, Atif.t2, Augman85, ClueBot, Mlspeten, Binksternet, The Thing That Should Not Be, Cambrasa, Enthusiast01, Ice77cool, Yamakiri, Alexbot, Diegocr, Abrech, Vivio Testarossa, Kihoiu, Dilumb, Rhododendrites, SchreiberBike, Wvithanage, Cyko 01, Classicrockfan42, ClanCC, Miami33139, XLinkBot, Mmv-ru, Petchboo, OWV, Cwilso, Harisankarh, Little Mountain 5, Cmr08, Lewu, Moose mangle, Harjk, Lajena, Addbot, Imeriki al-Shimoni, VCHunter, Qnext-Support, Tothwolf, Larrybowler, Cuaxdon, MrOllie, Jreconomy, ManiaQ, RogersMD, Jakester23jj, Evildeathmath, Tide rolls, Krano, Gail, SasiSasi, Vincent stehle, Arm-1234, Legobot, Yobot, Tohd8BohaithuGh1, Old Death, Dfe6543, Preston.lee, Knownot, RedMurcury1~enwiki, Koman90, AnomieBOT, Bwishon, Kristen Eriksen, Sonia, Dinesh smita, FenrirTheWolf, Neilapalmer, Materialscientist, CoMePrAdZ, Citation bot, Teilolondon, LilHelpa, MC707, Ludditesoft, Lairdp, Laboriousme, Mrdoomino, Tad Lincoln, Jmundo, Miym, Mobilon, Abce2, Frosted14, Kevinzhouyan, Zicko1, Felix.rivas, Bahahs, Coolblaze03, Alainr345, Shadowjams, Nyhet, Tknew, Dougofborg, FrescoBot, Sky Attacker, Sae1962, Eliezerb, Drew R. Smith, Tom235, Tiger Brown, Pinethicket, I dream of horses, Btrest, A8UDI, Gabrielgmendonca, Ocexyz, Patrickzuili, Shielazhang, CountZer0, TobeBot, Irvine.david, Vrenator, TBloemink, Stjones86, Jeffrd10, Tyofcore, Peacedance, XDnonameXD, RjwilmsiBot, TjBot, Offnfopt, Dangerousrave, Noodles-sb, Slon02, DASHBot, P2prules, EmausBot, Orphan Wiki, WikitanvirBot, Snied, Yoelzanger, Klbrain, K6ka, AvicBot, Juststreamit, Josve05a, MorbidEntree, Fred Gandt, Wayne Slam, Layona1, Donner60, Senator2029, DASHBotAV, Mattsenate, Rocketrod1960, Helpsome, Will Beback Auto, ClueBot NG, Jack Greenmaven, Lokeshyadav99, Satellizer, Mesoderm, BC108, Widr, G8yingri, Helpful Pixie Bot, Manja Neuhaus, Lowercase sigmabot, BG19bot, Desmarie17, Absalom23, Metricopolus, RentalicKim, Editerjhon, Skpande, Lesldock, Chazza1113, TRBurton, ChrisGualtieri, ZappaOMati, Ducknish, Profilemine, FoCuSandLeArN, Codename Lisa, Hmainsbot1, GrayEagle1, Nonnompow, Lugia2453, Rcomrce, Razibot, Epicgenius, Pronacampo9, Tigstep, Maxwell bernard, Nshunter, Cp123127, EvergreenFir, Cecilia Hecht, Sahil sharma2119, Myconix, Lesser Cartographies, Ginsuloft, Ekilson, AlyssaG92, CBCompton, J grider65, Cespo4, Ppcoinwikipeercoin, Jkielty82, Fixuture, Saectar, SwiftCrimson, Rosesollere, Hard ToOp, Drkhataniar, Monkbot, Cazer78, V-apharmd, Vanished user 31lk45mnzx90, MARIODOESBREAKFAST, W.phillips7, AkashValliath, Rademers, Emhohensee, Nelsonkam, Gautamdebjani, IPUpfficia, Jesuufamtobie, Astapor12, CAPTAIN RAJU, Saghiri-optimus and Anonymous: 1125

- **Proof-of-work system** *Source:* https://en.wikipedia.org/wiki/Proof-of-work_system?oldid=737783472 *Contributors:* Michael Hardy, Mike Linksvayer, Robbot, DataSurfer, Cloud200, Matt Crypto, Bender235, Lycurgus, Tromp, Pearle, Pgimeno~enwiki, Oleg Alexandrov, MarkSteward, Julian Krause, Rjwilmsi, Helvetius, Flarn2006, Bgwhite, John Quincy Adding Machine, Avalon, SmackBot, Jon513, Frap, Dreadstar, Jhonan, Nishkid64, Camilo Sanchez, CmdrObot, N2e, Acabtp, Kredal, Headbomb, JustAGal, Davidhorman, SeanTater, Albany NY, Magioladitis, NoDepositNoReturn, Yakushima, Logictheo, David Eppstein, Gwern, Ontarioboy, TreasuryTag, Giszmo~enwiki, Nicksh, Doublesuited, Mumiemonstret, SuzieDerkins, Chrisarnesen, Mehmud, Miami33139, XLinkBot, Addbot, AnomieBOT, DannyAsher, Omnipaedista, Breadblade, Jesse V., RjwilmsiBot, Joeyhewitt, Mmeijeri, Euloiix, Jonpatterns, H3llBot, L0ngpar1sh, Ipsign, 4368a, BG19bot, Cliff12345, 0x0F, Tuxayo, Wuchang, Me, Myself, and I are Here, Adam2us, Play Money for Dummies, PostScarcity, Omninonsense, Saectar, Unicodesnowman, YubbaDoo, Monkbot, MARIODOESBREAKFAST, FOXIBOX, Hannasnow, Vivi239, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, JonBobbie, GreenC bot and Anonymous: 59

- **SHA-2** *Source:* https://en.wikipedia.org/wiki/SHA-2?oldid=741000839 *Contributors:* Zundark, Paul Ebermann, Nealmcb, Haakon, Ciphergoth, Jeffq, Giftlite, DavidCary, Ds13, Markus Kuhn, Jason Quinn, Hgfernan, Indolering, ArnoldReinhold, Smyth, Kwamikagami, Sietse Snel, RoyBoy, SpeedyGonsales, LOL, Dionyziz, Rjwilmsi, Ysangkok, Intgr, 121a0012, Bgwhite, Peterl, Wavelength, Jkg, CFSworks, Dsmouse, Ospalh, Arthur Rubin, Cedar101, Caligatio, Yamaguchi□□, Thumperward, EncMstr, Sadads, Malbrain, Frap, Hl, PeterJeremy, Sjock, Brajonrondo, Byrnejb, Snorkelman, Geremia, Jesse Viviano, Ebrahim, NadirAli, Jm3, Mojo Hand, Dawnseeker2000, Widefox, D V S, Doca, Erxnmedia, Od1n, Geniac, Xoneca, Magioladitis, AVRS, Jspiegler, Maurice Carbonaro, Jesant13, Smite-Meister, Robertgreer, Quindraco, Rogerdpack, Andy Dingley, Cowlinator, Neil Smithline, Sfan00 IMG, JJuran, Netvope, Borneq, Sun Creator, GlasGhost, DavidRabahy, Delt01, Addbot, Mortense, Thomas.pornin, Grashoofd, Maslen, OlEnglish, Yobot, AnomieBOT, Citation bot, Aleph Infinity, Quebec99, Digiphi, Octotron, Omnipaedista, Krisztián Pintér, Ialbrekht, MathsPoetry, Fortdj33, Alxeedo, Mfwitten, John85, Jonesey95, Skyerise, Loresayer, Lotje, Timtempleton, TheInevitable, Noloader, Dewritech, RenamedUser01302013, Dcirovic, Quelrod, Nosebinary, Westley Turner, Rushless, Quondum, Jacosoft apps, Shnako, ClueBot NG, Proz, Nielsduif, Catlemur, Joefromrandb, Meganomic, Skoot13, Frietjes, Parsley1972, BG19bot, Jackbrear, Wkunkel, Maartenvanrooijen, Maver2909, Felidofractals, Tony Tan, Pboudra, Cliff12345, Cyberbot II, Napcae, AMRMHR, CuriousMind01, Nonnompow, Manishrw, Kotz, Skeuomorf, DD4235, Richieframe, Dwarvenux, Severyn.kozak, Ppcoinwikipeercoin, Willisius, Bad Dryer, CPU Terminator, ReadWriteWriteRead, Claw of Slime, Maciej Czyżewski, Enrique Santos L., TheMagikCow, CV9933, Megatherium, Kurousagi, ThePiGrepper, GreenC bot and Anonymous: 113
- **ANX (Hong Kong company)** *Source:* https://en.wikipedia.org/wiki/ANX_(Hong_Kong_company)?oldid=731305153 *Contributors:* BD2412, Vegaswikian, Bgwhite, Deku-shrub, Eclipsed, ONUnicorn, Casliber, Keith D, Onel5969, Mean as custard, BG19bot, Reddogsix, DPL bot, SJ Defender, John Marsh 701, Filedelinkerbot, Dsprc, Walterlipolyu, Sunmist, Asia bun, ww, Ste Sasi, Rodney Linder, Jackbtcjack, Jackbtcjack123, Wikiwikipeter, Brahiim123 and Anonymous: 4
- **BitInstant** *Source:* https://en.wikipedia.org/wiki/BitInstant?oldid=715132439 *Contributors:* Bearcat, Kdammers, Smyth, Andrewpmk, Geraldshields11, Malcolma, BiH, Narkstraws, Ccchambers, Kozuch, Magioladitis, JoeDeRose, Agyle, Lamro, Chrisarnesen, AnomieBOT, PabloCastellano, MusikAnimal, Erik.Bjareholt, Mogism, Cmannatt, Bmrg567, MasturbatingCow, Xrt6L, JexsterB312, Vdrey, MrGiantEditor, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 15
- **Bitstamp** *Source:* https://en.wikipedia.org/wiki/Bitstamp?oldid=725105994 *Contributors:* Roybadami, Edward, Bearcat, Rpyle731, Smyth, Benlisquare, Dialectric, Tamfang, Obiwankenobi, Magioladitis, Jhirsch41, Black Kite, Agyle, VanishedUser sdu9aya9fs787sads, Chrisarnesen, 4th-otaku, AnomieBOT, RevelationDirect, Sargdub, Atilla000, Emisanle, ChrisGualtieri, Citation Needed, Ildottoreverde, Wuerzele, Ginsuloft, Ssanchezd, Wolololol, PirateButtercup, Wasill37, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 10
- **BTC-e** *Source:* https://en.wikipedia.org/wiki/BTC-e?oldid=730564001 *Contributors:* Piotrus, Hierarchypedia, Eclipsed, AjaxSmack, TheCatalyst31, AnomieBOT, EmausBot, Compgenius, Bamyers99, GermanJoe, Satellizer, Wgolf, Emisanle, BG19bot, TranslucentCloud, Cyberbot II, 0x0F, Wolololol, RebelOfBabylon, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 2
- **BTC China** *Source:* https://en.wikipedia.org/wiki/BTC_China?oldid=714883106 *Contributors:* Pmsyyz, Anthony Appleyard, Benlisquare, Kozuch, Obiwankenobi, Malvineous, Magioladitis, Ontarioboy, Black Kite, Agyle, Chrisarnesen, C933103, I dream of horses, Sargdub, Citation Needed, Jamesmcmahon0, CNMall41, Wasill37, Chenyijia001, Jackbtcjack, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 2
- **Buttercoin** *Source:* https://en.wikipedia.org/wiki/Buttercoin?oldid=723679176 *Contributors:* BD2412, Black Falcon, Kozuch, Obiwankenobi, Vanished user ty12kl89jq10, DGG, Malik Shabazz, Agyle, Eeekster, Chrisarnesen, ZTebaykina, Yobot, BattyBot, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 5
- **Coinbase** *Source:* https://en.wikipedia.org/wiki/Coinbase?oldid=735953300 *Contributors:* Edward, Gabbe, Dbabbitt, Vipul, Sjö, Wjfox2005, Black Falcon, Egsan Bacon, Robofish, Nagle, N2e, Kozuch, Obiwankenobi, Magioladitis, Mercurywoodrose, Agyle, VanishedUser sdu9aya9fs787sads, ImageRemovalBot, Vishtany, Chrisarnesen, Gnickett1, Mortense, Download, 84user, Yobot, 4th-otaku, AnomieBOT, Ulric1313, Bliljerk101, Mean as custard, Sargdub, Dcirovic, Komodore, ClueBot NG, Jeraphine Gryphon, Mark Arsten, Cky2250, Cliff12345, BigButterfly, MarcoPolo419, Ascom99, Quenhitran, Makkachin, Sam Sailor, Jayaguru-Shishya, Xrt6L, Pinetreecrush, Gavleson, Bad Dryer, Infinitycoin, Josh DeBruycker, BitcoinWiki, I.eat.Gox, Gwlady, Spfcraze, Genegriff, Bdarmtrong, Daylen, Coinbasescam, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Brahiim123 and Anonymous: 34
- **Huobi** *Source:* https://en.wikipedia.org/wiki/Huobi?oldid=725131283 *Contributors:* Hierarchypedia, Eclipsed, Yobot, AnomieBOT, Foledman, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 2
- **ItBit** *Source:* https://en.wikipedia.org/wiki/ItBit?oldid=741349357 *Contributors:* Bearcat, David Gerard, Malcolma, Eclipsed, Black Falcon, Derek R Bullamore, Kozuch, Obiwankenobi, Magioladitis, Black Kite, Agyle, ChicagoRob78, Arjayay, Chrisarnesen, AnomieBOT, Sargdub, Slightsmile, Meatsgains, Citation Needed, Nv 225, Nyc10009, Itbit Exchange, Mrphobos123, ww, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Atlantic306, Natashagural and Anonymous: 4
- **LocalBitcoins** *Source:* https://en.wikipedia.org/wiki/LocalBitcoins?oldid=729558097 *Contributors:* Graeme Bartlett, GSK, Magioladitis, Bonadea, Black Kite, Chrisarnesen, Nickmeet, Dewritech, Jonpatterns, Jeraphine Gryphon, BG19bot, Daveman16, 0x0F, Citation Needed, Jerguismi, Sr.ganador, BitcoinUser, Chapipipopo, Peraurico, Ywecur, Liance, ToonLucas22 and Anonymous: 11
- **Mt. Gox** *Source:* https://en.wikipedia.org/wiki/Mt._Gox?oldid=739421010 *Contributors:* Edward, Delirium, Julesd, Timwi, Furrykef, SoWhy, DNewhall, AndrewKeenanRichardson, Thincat, Mike Rosoft, Shiftchange, Discospinster, Hydrox, Smyth, Deathawk, Officiallyover, SnowFire, Tabletop, Runarb, Fresheneesz, DVdm, Pburka, Resolute, Tweet, Ianmacm, Nagle, Optakeover, Norm mit, Kencf0618, Doceddi, Matthieu Houriet, Jesse Viviano, Gafter, Danrok, Medovina, Kozuch, PamD, Saintrain, Mojo Hand, Widefox, Obiwankenobi, Yellowdesk, Global Cerebral Ischemia, Kk5000, Acroterion, Magioladitis, Gwern, Maproom, Atama, Ajfweb, Maxxyme, Donjrude, B1db2, Agyle, CheloVechek, L32007, Jonahtrainer, SimonTrew, Svick, Trustable, Pianoman320, Trivialist, SkE, Chrisarnesen, NittyG, Tassedethe, Yobot, Mmacdon6, 4th-otaku, AnomieBOT, Hard700, Brightgalrs, Crookesmoor, Пилигрим, FrescoBot, Surv1v4l1st, Djetelina, Sjcjoosten, Stephanefr, Aoidh, Dewritech, Wikipelli, Dcirovic, K6ka, NicatronTg, Jack Sebastian, Brandmeister, Ego White Tray, ClueBot NG, Geoburke, Catlemur, Hpersh, Widr, Newyorkadam, Lowercase sigmabot,

BG19bot, McZusatz, Mark Arsten, Meatsgains, Blaspie55, Cliff12345, Shirudo, Grahvity, BattyBot, Cyberbot II, Esszet, Neoconfederate, Melonkelon, Soffredo, Wuerzele, ChaseAm, Brianen2, NorthBySouthBaranof, Makkachin, Tiban75, Bitkoof, Verjohnpike, Xrt6L, Vidmastb, Kubrixcube, Eliteware, Hakanwk, Aniapie, OKNoah, I.eat.Gox, Ross.PokerVIP, Mollyjohn1436, Ddoback, Liance, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Mbevand, GreenC bot and Anonymous: 77

- **OKCoin** *Source:* https://en.wikipedia.org/wiki/OKCoin?oldid=737936675 *Contributors:* BenM, Bgwhite, Deku-shrub, Timtrent, Magioladitis, StAnselm, XLinkBot, Yobot, AnomieBOT, LilHelpa, Sargdub, Newzack, Pastafarianist, BattyBot, Zekesonxx, Salvationist2nd, OKCoin, Rayna Jaymes, Redartsina, SAnthonyR, Eric Pode lives, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, AaronD9933 and Anonymous: 4

6.2 Images

- **File:10elqpi.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/93/10elqpi.jpg *License:* CC BY-SA 3.0 *Contributors:* Transferred from en.wikipedia to Commons. *Original artist:* The original uploader was Ladislav Mecir at English Wikipedia
- **File:ASICMINER_USB_Block_Erupter.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d3/ASICMINER_USB_Block_Erupter.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Targaryen
- **File:All-currency-symbol.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/9d/All-currency-symbol.svg *License:* Public domain *Contributors:* Own work *Original artist:* User:StalkerAT
- **File:Ambox_current_red.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/98/Ambox_current_red.svg *License:* CC0 *Contributors:* self-made, inspired by Gnome globe current event.svg, using Information icon3.svg and Earth clip art.svg *Original artist:* Vipersnake151, penubag, Tkgd2007 (clock)
- **File:Ambox_important.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/b4/Ambox_important.svg *License:* Public domain *Contributors:* Own work, based off of Image:Ambox scales.svg *Original artist:* Dsmurat (talk · contribs)
- **File:AustrianBitCoinMiningRig.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/6/6c/AustrianBitCoinMiningRig.jpg *License:* CC BY 2.0 *Contributors:* https://secure.flickr.com/photos/gastev/8157565917 *Original artist:* Gastev (Mirko Tobias Schaefer)
- **File:Avalon-An_ASIC_base_bitcoin_machine.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/e/ee/Avalon-An_ASIC_base_bitcoin_machine.jpg *License:* CC0 *Contributors:* Sent to me personally *Original artist:* □□□
- **File:BTC_number_of_transactions_per_month.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/c8/BTC_number_of_transactions_per_month.png *License:* CC0 *Contributors:* Own work *Original artist:* Zhitelew
- **File:Bitcoin.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/46/Bitcoin.svg *License:* CC0 *Contributors:* This file was derived from: Bitcoin logo.svg
  Original artist: Bitboy
- **File:BitcoinATM.JPG** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f6/BitcoinATM.JPG *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* KennethHan
- **File:BitcoinSign.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/ba/BitcoinSign.svg *License:* Public domain *Contributors:* http://bitcoin.org *Original artist:* Satoshi Nakamoto
- **File:Bitcoin_ATM_in_Vienna.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/40/Bitcoin_ATM_in_Vienna.jpg *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Elph
- **File:Bitcoin_Transaction_Visual.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/ce/Bitcoin_Transaction_Visual.svg *License:* CC0 *Contributors:* Inkscape
  Previously published: https://github.com/graingert/bitcoin-IRP/blob/master/img/Bitcoin_Transaction_Visual.svg *Original artist:* Graingert
- **File:Bitcoin_exchange_mtgox_-_Feb2012-Feb2014_-_log_scale.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/99/Bitcoin_exchange_mtgox_-_Feb2012-Feb2014_-_log_scale.png *License:* CC BY-SA 3.0 *Contributors:* http://bitcoincharts.com/charts/mtgoxUSD#rg730zigDailyztgMzm1g10zm2g25zl *Original artist:* http://bitcoincharts.com
- **File:Bitcoin_logo.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/c5/Bitcoin_logo.svg *License:* CC0 *Contributors:* Bitcoin forums *Original artist:* Bitboy
- **File:Bitcoin_paper_wallet_generated_at_bitaddress.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/db/Bitcoin_paper_wallet_generated_at_bitaddress.jpg *License:* MIT *Contributors:* http://bitaddress.org *Original artist:* Open Source
- **File:Bitcoin_price_and_volatility.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/d/d5/Bitcoin_price_and_volatility.svg *License:* CC-BY-SA-3.0 *Contributors:*

  Own work - Data source: Blockchain.info, created in LibreOffice Calc

  Original artist:

  Ladislav (talk) (Uploads)
- **File:Bitcoinpaymentverification.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/2/24/Bitcoinpaymentverification.png *License:* MIT *Contributors:* http://bitcoin.org/bitcoin.pdf *Original artist:* Satoshi Nakamoto
- **File:BitstampUSD_weekly.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/92/BitstampUSD_weekly.png *License:* CC BY-SA 3.0 *Contributors:* http://bitcoincharts.com/charts/bitstampUSD#rg730zigWeeklyztgTzm1g10zm2g10zl *Original artist:* Bitcoin Charts
- **File:Bitstamp_Logo_2013.png** *Source:* https://upload.wikimedia.org/wikipedia/en/6/68/Bitstamp_Logo_2013.png *License:* Fair use *Contributors:* http://www.thebitcoinchannel.com/archives/12355 *Original artist:* ?
- **File:Blockchain.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/98/Blockchain.svg *License:* CC BY 3.0 *Contributors:* Bitcoin Wiki: https://en.bitcoin.it/wiki/File:Blockchain.png *Original artist:*

  - original file: Theymos from Bitcoin wiki
  - vectorization: Own work

- **File:Buttercoin_Logo_LowRes.png** *Source:* https://upload.wikimedia.org/wikipedia/en/3/38/Buttercoin_Logo_LowRes.png *License:* Fair use *Contributors:* Buttercoin official website: http://www.buttercoin.com/#/ *Original artist:* ?
- **File:Butterfly_Labs_60GH_Bitcoin_Miner_Single_SC.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/0/04/Butterfly_Labs_60GH_Bitcoin_Miner_Single_SC.jpg *License:* CC BY-SA 3.0 *Contributors:* https://forums.butterflylabs.com/dbtgallery.php?do=view_image&id=1169&gal=gallery *Original artist:* Joshua Zerlan
- **File:Cameron_Winklevoss_at_the_2008_Beijing_Olympics_-_20080817.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/76/Cameron_Winklevoss_at_the_2008_Beijing_Olympics_-_20080817.jpg *License:* CC BY 3.0 *Contributors:* Own work. *Original artist:* Johnnyroee.
- **File:Cash_template.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/19/Cash_template.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Ain92
- **File:Coinbase_Logo_2013.png** *Source:* https://upload.wikimedia.org/wikipedia/en/c/c7/Coinbase_Logo_2013.png *License:* Fair use *Contributors:* https://www.facebook.com/Coinbase *Original artist:* ?
- **File:Commons-logo.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/4/4a/Commons-logo.svg *License:* CC-BY-SA-3.0 *Contributors:* ? *Original artist:* ?
- **File:Crypto_key.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/6/65/Crypto_key.svg *License:* CC-BY-SA-3.0 *Contributors:* Own work based on image:Key-crypto-sideways.png by MisterMatt originally from English Wikipedia *Original artist:* MesserWoland
- **File:Cryptocurrency_Mining_Farm.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/37/Cryptocurrency_Mining_Farm.jpg *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Marco Krohn
- **File:Crystal_Clear_app_browser.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/fe/Crystal_Clear_app_browser.png *License:* LGPL *Contributors:* All Crystal icons were posted by the author as LGPL on kde-look *Original artist:* Everaldo Coelho and YellowIcon
- **File:DHT_en.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/98/DHT_en.svg *License:* Public domain *Contributors:* Jnlin *Original artist:* Jnlin
- **File:De_Waag_Bitcoin.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/cd/De_Waag_Bitcoin.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Targaryen
- **File:Desktop_computer_clipart_-_Yellow_theme.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d7/Desktop_computer_clipart_-_Yellow_theme.svg *License:* CC0 *Contributors:* https://openclipart.org/detail/17924/computer *Original artist:* AJ from openclipart.org
- **File:Edit-clear.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/f/f2/Edit-clear.svg *License:* Public domain *Contributors:* The *Tango! Desktop Project*. *Original artist:*

  The people from the Tango! project. And according to the meta-data in the file, specifically: “Andreas Nilsson, and Jakub Steiner (although minimally).”
- **File:Electrum_Bitcoin_Wallet.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/16/Electrum_Bitcoin_Wallet.png *License:* GPL *Contributors:* http://electrum.org/ *Original artist:* electrum
- **File:Emblem-money.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f3/Emblem-money.svg *License:* GPL *Contributors:* http://www.gnome-look.org/content/show.php/GNOME-colors?content=82562 *Original artist:* perfectska04
- **File:Estimated-transaction-volume-usd.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/5/57/Estimated-transaction-volume-usd.svg *License:* CC0 *Contributors:* Own work *Original artist:* Ladislav Mecir
- **File:Flag_of_Argentina.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/1a/Flag_of_Argentina.svg *License:* Public domain *Contributors:* Here, based on: http://manuelbelgrano.gov.ar/bandera/creacion-de-la-bandera-nacional/ *Original artist:* Government of Argentina
- **File:Flag_of_Australia.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/b/b9/Flag_of_Australia.svg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Bangladesh.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f9/Flag_of_Bangladesh.svg *License:* Public domain *Contributors:* http://www.dcaa.com.bd/Modules/CountryProfile/BangladeshFlag.aspx *Original artist:* User:SKopp
- **File:Flag_of_Belgium_(civil).svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/92/Flag_of_Belgium_%28civil%29.svg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Bolivia.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/48/Flag_of_Bolivia.svg *License:* Public domain *Contributors:* Own work *Original artist:* User:SKopp
- **File:Flag_of_Brazil.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/0/05/Flag_of_Brazil.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Bulgaria.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/9a/Flag_of_Bulgaria.svg *License:* Public domain *Contributors:* The flag of Bulgaria. The colors are specified at http://www.government.bg/cgi-bin/e-cms/vis/vis.pl?s=001&p=0034&n=000005&g= as: *Original artist:* SKopp
- **File:Flag_of_Canada.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/c/cf/Flag_of_Canada.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Chile.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/78/Flag_of_Chile.svg *License:* Public domain *Contributors:* Own work *Original artist:* SKopp
- **File:Flag_of_Colombia.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/2/21/Flag_of_Colombia.svg *License:* Public domain *Contributors:* Drawn by User:SKopp *Original artist:* SKopp

- **File:Flag_of_Croatia.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/1b/Flag_of_Croatia.svg *License:* Public domain *Contributors:* http://www.sabor.hr/Default.aspx?sec=4317 *Original artist:* Nightstallion, Elephantus, Neoneo13, Denelson83, Rainman, R-41, Minestrone, Lupo, Zscout370,
  <a href='//commons.wikimedia.org/wiki/User:MaGa' title='User:MaGa'>**Ma**</a><a href='//commons.wikimedia.org/wiki/File:Croatian_squares_Ljubicic.png' class='image'><img alt='Croatian squares Ljubicic.png' src='https://upload.wikimedia.org/wikipedia/commons/thumb/7/7f/Croatian_squares_Ljubicic.png/15px-Croatian_squares_Ljubicic.png' width='15' height='15' srcset='https://upload.wikimedia.org/wikipedia/commons/thumb/7/7f/Croatian_squares_Ljubicic.png/23px-Croatian_squares_Ljubicic.png 1.5x, https://upload.wikimedia.org/wikipedia/commons/thumb/7/7f/Croatian_squares_Ljubicic.png/30px-Croatian_squares_Ljubicic.png 2x' data-file-width='202' data-file-height='202' /></a><a href='//commons.wikimedia.org/wiki/User_talk:MaGa' title='User talk:MaGa'>**Ga**</a> (based on Decision of the Parliament)
- **File:Flag_of_Cyprus.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d4/Flag_of_Cyprus.svg *License:* Public domain *Contributors:* Own work *Original artist:* User:Vzb83
- **File:Flag_of_Denmark.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/9c/Flag_of_Denmark.svg *License:* Public domain *Contributors:* Own work *Original artist:* User:Madden
- **File:Flag_of_Ecuador.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/e/e8/Flag_of_Ecuador.svg *License:* Public domain *Contributors:* http://www.presidencia.gob.ec/pdf/Simbolos-Patrios.pdf *Original artist:* President of the Republic of Ecuador, Zscout370
- **File:Flag_of_Estonia.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/8/8f/Flag_of_Estonia.svg *License:* Public domain *Contributors:* http://www.riigikantselei.ee/?id=73847 *Original artist:* Originally drawn by User:SKopp. Blue colour changed by User:PeepP to match the image at [1].
- **File:Flag_of_Europe.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/b7/Flag_of_Europe.svg *License:* Public domain *Contributors:*
- File based on the specification given at [1]. *Original artist:* User:Verdy p, User:-xfi-, User:Paddu, User:Nightstallion, User:Funakoshi, User:Jeltz, User:Dbenbenn, User:Zscout370
- **File:Flag_of_Finland.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/bc/Flag_of_Finland.svg *License:* Public domain *Contributors:* http://www.finlex.fi/fi/laki/ajantasa/1978/19780380 *Original artist:* Drawn by User:SKopp
- **File:Flag_of_France.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/c/c3/Flag_of_France.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Germany.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/b/ba/Flag_of_Germany.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Greece.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/5/5c/Flag_of_Greece.svg *License:* Public domain *Contributors:* own code *Original artist:* (of code) cs:User:-xfi- (talk)
- **File:Flag_of_Hong_Kong.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/5/5b/Flag_of_Hong_Kong.svg *License:* Public domain *Contributors:* http://www.protocol.gov.hk/flags/chi/r_flag/index.html *Original artist:* Tao Ho
- **File:Flag_of_Iceland.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/ce/Flag_of_Iceland.svg *License:* Public domain *Contributors:* Islandic National Flag *Original artist:* Ævar Arnfjörð Bjarmason, Zscout370 and others
- **File:Flag_of_India.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/4/41/Flag_of_India.svg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Indonesia.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/9f/Flag_of_Indonesia.svg *License:* Public domain *Contributors:* Law: s:id:Undang-Undang Republik Indonesia Nomor 24 Tahun 2009 (http://badanbahasa.kemdiknas.go.id/lamanbahasa/sites/default/files/UU_2009_24.pdf) *Original artist:* Drawn by User:SKopp, rewritten by User:Gabbe
- **File:Flag_of_Ireland.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/45/Flag_of_Ireland.svg *License:* Public domain *Contributors:* Drawn by User:SKopp *Original artist:* ?
- **File:Flag_of_Israel.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d4/Flag_of_Israel.svg *License:* Public domain *Contributors:* http://www.mfa.gov.il/MFA/History/Modern%20History/Israel%20at%2050/The%20Flag%20and%20the%20Emblem *Original artist:* “The Provisional Council of State Proclamation of the Flag of the State of Israel” of 25 Tishrei 5709 (28 October 1948) provides the official specification for the design of the Israeli flag.
- **File:Flag_of_Italy.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/0/03/Flag_of_Italy.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Japan.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/9/9e/Flag_of_Japan.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Jordan.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/c0/Flag_of_Jordan.svg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Kyrgyzstan.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/c7/Flag_of_Kyrgyzstan.svg *License:* Public domain *Contributors:* Drawn by User:SKopp, construction sheet. Redo by: cs:User:-xfi- *Original artist:* Made by Andrew Duhan for the Sodipodi SVG flag collection, and is public domain.
- **File:Flag_of_Lebanon.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/5/59/Flag_of_Lebanon.svg *License:* Public domain *Contributors:* ? *Original artist:* Traced based on the CIA World Factbook with some modification done to the colours based on information at Vexilla mundi.
- **File:Flag_of_Lithuania.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/11/Flag_of_Lithuania.svg *License:* Public domain *Contributors:* Own work *Original artist:* SuffKopp
- **File:Flag_of_Luxembourg.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/da/Flag_of_Luxembourg.svg *License:* Public domain *Contributors:* Own work http://www.legilux.public.lu/leg/a/archives/1972/0051/a051.pdf#page=2, colors from http://www.legilux.public.lu/leg/a/archives/1993/0731609/0731609.pdf *Original artist:* Drawn by User:SKopp

- **File:Flag_of_Malaysia.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/6/66/Flag_of_Malaysia.svg *License:* Public domain *Contributors:* Create based on the Malaysian Government Website (archive version)
Original artist: SKopp, Zscout370 and Ranking Update

- **File:Flag_of_Malta.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/73/Flag_of_Malta.svg *License:* CC0 *Contributors:* ? *Original artist:* ?
- **File:Flag_of_New_Zealand.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/3e/Flag_of_New_Zealand.svg *License:* Public domain *Contributors:* http://www.mch.govt.nz/files/NZ%20Flag%20-%20proportions.JPG *Original artist:* Zscout370, Hugh Jass and many others
- **File:Flag_of_Nicaragua.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/19/Flag_of_Nicaragua.svg *License:* Public domain *Contributors:* Own work based on: <a data-x-rel='nofollow' class='external text' href='https://docs.google.com/viewer?a=v,<span>,&,</span>,q=cache:tRiqYRg_YJ4J:www.casc.gob.ni/index.php?option%3Dcom_docman%26task%3Ddoc_download%26gid%3D704%26Itemid%3D4+ley+sobre+los+simbolo+patrios+nicaragua+2002,<span>,&,</span>,hl=es,<span>,&,</span>,gl=ni,<span>,&,</span>,pid=bl,<span>,&,</span>,srcid=ADGEEShaqFptSDRqZyUoeWlWgMGTvcFvWOs
About Characteristics And Use Of Patriotic Symbols of Nicaragua</a> *Original artist:* C records (talk · contribs)
- **File:Flag_of_Norway.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d9/Flag_of_Norway.svg *License:* Public domain *Contributors:* Own work *Original artist:* Dbenbenn
- **File:Flag_of_Pakistan.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/32/Flag_of_Pakistan.svg *License:* Public domain *Contributors:* The drawing and the colors were based from flagspot.net. *Original artist:* User:Zscout370
- **File:Flag_of_Poland.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/1/12/Flag_of_Poland.svg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Portugal.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/5/5c/Flag_of_Portugal.svg *License:* Public domain *Contributors:* http://jorgesampaio.arquivo.presidencia.pt/pt/republica/simbolos/bandeiras/index.html#imgs *Original artist:* Columbano Bordalo Pinheiro (1910; generic design); Vítor Luís Rodrigues; António Martins-Tuválkin (2004; this specific vector set: see sources)
- **File:Flag_of_Romania.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/73/Flag_of_Romania.svg *License:* Public domain *Contributors:* Own work *Original artist:* AdiJapan
- **File:Flag_of_Russia.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/f/f3/Flag_of_Russia.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Singapore.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/48/Flag_of_Singapore.svg *License:* Public domain *Contributors:* The drawing was based from http://app.www.sg/who/42/National-Flag.aspx. Colors from the book: *(2001). The National Symbols Kit. Singapore: Ministry of Information, Communications and the Arts. pp. 5. ISBN 8880968010* Pantone 032 shade from http://www.pantone.com/pages/pantone/colorfinder.aspx?c_id=13050 *Original artist:* Various
- **File:Flag_of_Slovakia.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/e/e6/Flag_of_Slovakia.svg *License:* Public domain *Contributors:* Own work; here, colors *Original artist:* SKopp
- **File:Flag_of_Slovenia.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f0/Flag_of_Slovenia.svg *License:* Public domain *Contributors:* Own work construction sheet from http://flagspot.net/flags/si%27.html#coa *Original artist:* User:Achim1999
- **File:Flag_of_South_Africa.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/af/Flag_of_South_Africa.svg *License:* Public domain *Contributors:* Per specifications in the Constitution of South Africa, Schedule 1 - National flag *Original artist:* Flag design by Frederick Brownell, image by Wikimedia Commons users
- **File:Flag_of_South_Korea.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/0/09/Flag_of_South_Korea.svg *License:* Public domain *Contributors:* Ordinance Act of the Law concerning the National Flag of the Republic of Korea, Construction and color guidelines (Russian/English) *Original artist:* Various
- **File:Flag_of_Spain.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/9/9a/Flag_of_Spain.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Sweden.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/4/4c/Flag_of_Sweden.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Flag_of_Switzerland.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f3/Flag_of_Switzerland.svg *License:* Public domain *Contributors:* PDF Colors Construction sheet *Original artist:* User:Marc Mongenet

Credits:

- **File:Flag_of_Thailand.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/a9/Flag_of_Thailand.svg *License:* Public domain *Contributors:* Own work *Original artist:* Zscout370
- **File:Flag_of_Turkey.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/b4/Flag_of_Turkey.svg *License:* Public domain *Contributors:* Turkish Flag Law (Türk Bayrağı Kanunu), Law nr. 2893 of 22 September 1983. Text (in Turkish) at the website of the Turkish Historical Society (Türk Tarih Kurumu) *Original artist:* David Benbennick (original author)
- **File:Flag_of_Vietnam.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/2/21/Flag_of_Vietnam.svg *License:* Public domain *Contributors:* http://vbqppl.moj.gov.vn/law/vi/1951_to_1960/1955/195511/195511300001 http://vbqppl.moj.gov.vn/vbpq/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=820 *Original artist:* Lưu Ly vẽ lại theo nguồn trên
- **File:Flag_of_the_Czech_Republic.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/cb/Flag_of_the_Czech_Republic.svg *License:* Public domain *Contributors:*
  - -xfi-'s file
  - -xfi-'s code
  - Zirland's codes of colors

Original artist:

(of code): SVG version by cs:-xfi-.

- **File:Flag_of_the_Netherlands.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/2/20/Flag_of_the_Netherlands.svg *License:* Public domain *Contributors:* Own work *Original artist:* Zscout370
- **File:Flag_of_the_People'{}s_Republic_of_China.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/fa/Flag_of_the_People%27s_Republic_of_China.svg *License:* Public domain *Contributors:* Own work, http://www.protocol.gov.hk/flags/eng/n_flag/design.html *Original artist:* Drawn by User:SKopp, redrawn by User:Denelson83 and User:Zscout370
- **File:Flag_of_the_Philippines.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/99/Flag_of_the_Philippines.svg *License:* Public domain *Contributors:* The design was taken from [1] and the colors were also taken from a Government website *Original artist:* User:Achim1999
- **File:Flag_of_the_Republic_of_China.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/72/Flag_of_the_Republic_of_China.svg *License:* Public domain *Contributors:* [1] *Original artist:* User:SKopp
- **File:Flag_of_the_United_Kingdom.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/a/ae/Flag_of_the_United_Kingdom.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Flag_of_the_United_States.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/a/a4/Flag_of_the_United_States.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Folder_Hexagonal_Icon.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/4/48/Folder_Hexagonal_Icon.svg *License:* Cc-by-sa-3.0 *Contributors:* ? *Original artist:* ?
- **File:Free-to-read_lock_75.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/8/80/Free-to-read_lock_75.svg *License:* CC0 *Contributors:* Adapted from 9px|Open_Access_logo_PLoS_white_green.svg *Original artist:* This version:Trappist_the_monk (talk) (Uploads)
- **File:Free_and_open-source_software_logo_(2009).svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/31/Free_and_open-source_software_logo_%282009%29.svg *License:* Public domain *Contributors:* FOSS Logo.svg *Original artist:* Free Software Portal Logo.svg (FOSS Logo.svg): ViperSnake151
- **File:History_of_Bitcoin_difficulty.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/4b/History_of_Bitcoin_difficulty.svg *License:* BSD *Contributors:* Own work *Original artist:* Ladislav (talk) (Uploads)
- **File:Imbox_content.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/38/Imbox_content.png *License:* PD *Contributors:*

  Derived from Image:Information icon.svg *Original artist:*

  El T (original icon); David Levy (modified design); Penubag (modified color)
- **File:Lancelot-A_FPGA_based_bitcoin_mining_board.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f0/Lancelot-A_FPGA_based_bitcoin_mining_board.jpg *License:* CC0 *Contributors:* Sent to me personally *Original artist:* □□□
- **File:MtGox.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/dc/MtGox.png *License:* Public domain *Contributors:* MtGox.com *Original artist:* MtGox
- **File:Office-book.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/a8/Office-book.svg *License:* Public domain *Contributors:* This and myself. *Original artist:* Chris Down/Tango project
- **File:P2P-network.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/3f/P2P-network.svg *License:* Public domain *Contributors:* Own work *Original artist:* User:Mauro Bieg
- **File:People_icon.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/37/People_icon.svg *License:* CC0 *Contributors:* OpenClipart *Original artist:* OpenClipart
- **File:Portal-puzzle.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/f/fd/Portal-puzzle.svg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Proof_of_Work_challenge_response.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/5/55/Proof_of_Work_challenge_response.svg *License:* Public domain *Contributors:* Own work by the original uploader *Original artist:* Fabien Coelho (http://www.coelho.net/)
- **File:Proof_of_Work_solution_verification.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/2/24/Proof_of_Work_solution_verification.svg *License:* Public domain *Contributors:* Own work by the original uploader *Original artist:* Fabien Coelho (http://www.coelho.net/)
- **File:Question_book-new.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/9/99/Question_book-new.svg *License:* Cc-by-sa-3.0 *Contributors:*

  Created from scratch in Adobe Illustrator. Based on Image:Question book.png created by User:Equazcion *Original artist:*

  Tkgd2007
- **File:SHA-2.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/7d/SHA-2.svg *License:* CC-BY-SA-3.0 *Contributors:* Own work *Original artist:* User:kockmeyer
- **File:Server-based-network.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/fb/Server-based-network.svg *License:* LGPL *Contributors:* derived from the Image:Computer n screen.svg which is under the GNU LGPL *Original artist:* User:Mauro Bieg
- **File:Structured_(DHT)_peer-to-peer_network_diagram.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/79/Structured_%28DHT%29_peer-to-peer_network_diagram.png *License:* CC0 *Contributors:* Inkscape *Original artist:* Mesoderm
- **File:Symbol_book_class2.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/8/89/Symbol_book_class2.svg *License:* CC BY-SA 2.5 *Contributors:* Mad by Lokal_Profil by combining: *Original artist:* Lokal_Profil
- **File:Symbol_list_class.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/d/db/Symbol_list_class.svg *License:* Public domain *Contributors:* ? *Original artist:* ?

- **File:Text_document_with_red_question_mark.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/a4/Text_document_with_red_question_mark.svg *License:* Public domain *Contributors:* Created by bdesham with Inkscape; based upon Text-x-generic.svg from the Tango project. *Original artist:* Benjamin D. Esham (bdesham)
- **File:The_logo_of_OKCoin,_a_Chinese_bitcoin_exchange.png** *Source:* https://upload.wikimedia.org/wikipedia/en/c/ca/The_logo_of_OKCoin%2C_a_Chinese_bitcoin_exchange.png *License:* Fair use *Contributors:* OKCoin.com *Original artist:* ?
- **File:Torrentcomp_small.gif** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/3d/Torrentcomp_small.gif *License:* CC-BY-SA-3.0 *Contributors:* https://en.wikipedia.org/wiki/BitTorrent → smaller file-size GIF for BitTorrent article, cleaned up the dithered and ugly pixels. I made this to replace the monstrous 1.77 MB GIF residing on that article’s page. *Original artist:* Wikiadd
- **File:Total-bitcoins.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/e/ed/Total-bitcoins.svg *License:* CC-BY-SA-3.0 *Contributors:* ? *Original artist:* ?
- **File:TylerWinklevoss.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/9c/TylerWinklevoss.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* GabrielF
- **File:USB_Erupter.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/e/ec/USB_Erupter.jpg *License:* CC0 *Contributors:* Own work *Original artist:* FML
- **File:Unbalanced_scales.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/fe/Unbalanced_scales.svg *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:United_States_penny,_obverse,_2002.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/46/United_States_penny%2C_obverse%2C_2002.png *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Unstructured_peer-to-peer_network_diagram.png** *Source:* https://upload.wikimedia.org/wikipedia/en/f/fa/Unstructured_peer-to-peer_network_diagram.png *License:* CC0 *Contributors:*

  Inkscape

  Original artist:

  Mesoderm
- **File:V0cgp31.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/e/e5/V0cgp31.jpg *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Dertyqwerty
- **File:Wiki_letter_w_cropped.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/1c/Wiki_letter_w_cropped.svg *License:* CC-BY-SA-3.0 *Contributors:* This file was derived from Wiki letter w.svg: <a href='//commons.wikimedia.org/wiki/File:Wiki_letter_w.svg' class='image'><img alt='Wiki letter w.svg' src='https://upload.wikimedia.org/wikipedia/commons/thumb/6/6c/Wiki_letter_w.svg/50px-Wiki_letter_w.svg.png' width='50' height='50' srcset='https://upload.wikimedia.org/wikipedia/commons/thumb/6/6c/Wiki_letter_w.svg/75px-Wiki_letter_w.svg.png 1.5x, https://upload.wikimedia.org/wikipedia/commons/thumb/6/6c/Wiki_letter_w.svg/100px-Wiki_letter_w.svg.png 2x' data-file-width='44' data-file-height='44' /></a>
  Original artist: Derivative work by Thumperward
- **File:Yacy-resultados.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f1/Yacy-resultados.png *License:* GFDL *Contributors:* Trabajo propio/captura de pantalla *Original artist:* User:Hack-Master

6.3 Content license

- Creative Commons Attribution-Share Alike 3.0