

Cryptocurrencies

Contents

1	SHA-256-based	1
1.1	Bitcoin	1
1.1.1	Design	1
1.1.2	History	7
1.1.3	Economics	9
1.1.4	Legal status and regulation	15
1.1.5	Criminal activity	15
1.1.6	Security	18
1.1.7	Alternative applications of the block chain	19
1.1.8	Data in the block chain	19
1.1.9	In academia	19
1.1.10	In art, entertainment, and media	20
1.1.11	Bibliography	20
1.1.12	See also	21
1.1.13	Notes	21
1.1.14	References	22
1.1.15	External links	36
1.2	Mastercoin	36
1.2.1	References	36
1.2.2	External links	37
1.3	MazaCoin	37
1.3.1	References	37
1.3.2	External links	38
1.4	Namecoin	38
1.4.1	Records	38
1.4.2	Uses	38
1.4.3	History	39
1.4.4	See also	39
1.4.5	References	39
1.4.6	External links	40
1.5	NuBits	41
1.5.1	Notes	41

1.5.2	References	41
1.5.3	External links	41
1.6	Peercoin	41
1.6.1	Transactions	42
1.6.2	Creation of New Coins	42
1.6.3	Distinguishing features	42
1.6.4	Other	43
1.6.5	See also	43
1.6.6	References	43
1.6.7	External links	44
1.7	Bitcoin	44
1.7.1	History	44
1.7.2	Specifications	45
1.7.3	Awards and Recognition	45
1.7.4	Other adult cryptocurrencies	45
1.7.5	External links	45
1.7.6	References	45
2	Script-based	47
2.1	Auroracoin	47
2.1.1	History	47
2.1.2	Controversy	48
2.1.3	References	48
2.1.4	External links	49
2.2	Coinye	49
2.2.1	Release	49
2.2.2	Trademark infringement lawsuit	49
2.2.3	Developer departure and community takeover	49
2.2.4	Decline of use	49
2.2.5	External links	49
2.2.6	References	50
2.3	Dogecoin	51
2.3.1	Overview and history	51
2.3.2	Fundraising	52
2.3.3	Use and exchanges	53
2.3.4	Transactions	53
2.3.5	Mining parameters	53
2.3.6	Block schedule	54
2.3.7	Currency supply	54
2.3.8	References	54
2.3.9	External links	57
2.4	Litecoin	57

2.4.1	History	57
2.4.2	Development	57
2.4.3	Differences from Bitcoin	58
2.4.4	Transactions	58
2.4.5	Wallets	58
2.4.6	Exchanges	59
2.4.7	See also	59
2.4.8	References	59
2.4.9	External links	59
2.5	PotCoin	60
2.5.1	History	60
2.5.2	Overview and specification	60
2.5.3	Usage	60
2.5.4	Charitable fundraising	61
2.5.5	References	62
3	CryptoNote-based	63
3.1	CryptoNote	63
3.1.1	Origins	63
3.1.2	Anonymous transactions and ring signatures	64
3.1.3	Double spending protection	64
3.1.4	Egalitarian proof of work	65
3.1.5	Adaptive network limits	65
3.1.6	Philosophy	65
3.1.7	Current CryptoNote currencies	65
3.1.8	Controversy and criticism	69
3.1.9	See also	70
3.1.10	References	70
3.2	Monero (cryptocurrency)	72
3.2.1	History	72
3.2.2	Features	73
3.2.3	Usage	74
3.2.4	Limitations	74
3.2.5	Ongoing work and side projects	74
3.2.6	Applications	74
3.2.7	See also	75
3.2.8	External links	75
3.2.9	References	75
4	Other proof-of-work	77
4.1	Dash (cryptocurrency)	77
4.1.1	Overview	77

4.1.2	History	78
4.1.3	References	79
4.1.4	External links	79
4.2	Primecoin	79
4.2.1	Features	80
4.2.2	Proof-of-work system	80
4.2.3	See also	80
4.2.4	References	81
4.2.5	External links	81
4.3	Ethereum	81
4.3.1	Purpose	82
4.3.2	Development	82
4.3.3	Ether	82
4.3.4	Contracts	82
4.3.5	Implementations	83
4.3.6	Media	83
4.3.7	References	83
4.3.8	External links	84
5	Non proof-of-work	85
5.1	BlackCoin	85
5.1.1	Proof-of-Stake	85
5.1.2	Merchant adoption	85
5.1.3	See also	85
5.1.4	References	85
5.1.5	External links	86
5.2	Counterparty (technology)	86
5.2.1	XCP	86
5.2.2	Assets	86
5.2.3	Decentralized Exchange (DEX)	89
5.2.4	Software	89
5.2.5	Notable assets and issuers	90
5.2.6	Block Explorers	91
5.2.7	References	91
5.2.8	External links	92
5.3	NEM (cryptocurrency)	93
5.3.1	History	93
5.3.2	Development	93
5.3.3	Unique features	93
5.3.4	External links	95
5.3.5	References	95
5.4	Nxt	96

5.4.1	History	96
5.4.2	Concept	96
5.4.3	Features	97
5.4.4	Criticism	99
5.4.5	3rd Party use	100
5.4.6	See also	100
5.4.7	References	100
5.4.8	External links	101
5.5	Ripple (payment protocol)	101
5.5.1	History	101
5.5.2	Concept	103
5.5.3	Design features	103
5.5.4	XRP	106
5.5.5	Reception	107
5.5.6	See also	107
5.5.7	References	107
5.5.8	Further reading	111
5.5.9	External links	111
5.6	Stellar (payment network)	111
5.6.1	Design	111
5.6.2	Real-world Applications of Stellar	111
5.6.3	Stellar Consensus Protocol	112
5.6.4	References	112
5.6.5	Other websites	113
6	The technology	114
6.1	Block chain (database)	114
6.1.1	Name	114
6.1.2	Basic principles	114
6.1.3	Decentralisation	115
6.1.4	Token-less block chain debate	115
6.1.5	Data storage	115
6.1.6	Bitcoin sidechain implementations	115
6.1.7	Alternative chain designs	116
6.1.8	See also	116
6.1.9	References	116
6.2	Cryptocurrency tumbler	117
6.2.1	Alternative implementations	118
6.2.2	References	118
6.3	Proof-of-stake	118
6.3.1	Block Selection Variants	118
6.3.2	Advantages	119

6.3.3	Criticism	119
6.3.4	See also	120
6.3.5	References	120
6.4	Proof-of-work system	121
6.4.1	Background	121
6.4.2	Variants	121
6.4.3	List of proof-of-work functions	122
6.4.4	Reusable proof-of-work as e-money	123
6.4.5	Notes	123
6.4.6	See also	123
6.4.7	References	123
6.4.8	External links	124
6.5	Zerocoin	124
6.5.1	Rationale	125
6.5.2	Zerocoin protocol	125
6.5.3	Moneta	126
6.5.4	Criticism	126
6.5.5	Zerocash	126
6.5.6	Bear Bonds	126
6.5.7	References	126
6.5.8	External links	127
7	Text and image sources, contributors, and licenses	128
7.1	Text	128
7.2	Images	132
7.3	Content license	135

Chapter 1

SHA-256-based

1.1 Bitcoin

Bitcoin^{[note 5][note 6]} is a digital asset^[15] and a payment system invented by Satoshi Nakamoto,^[note 7] who published the invention in 2008^[11] and released it as open-source software in 2009.^[17] The system is peer-to-peer; users can transact directly without an intermediary.^{[18]:4} Transactions are verified by network nodes and recorded in a public distributed ledger called the *block chain*.^[19] The ledger uses bitcoin as its unit of account. The system works without a central repository or single administrator, which has led the U.S. Treasury to categorize bitcoin as a decentralized virtual currency.^[1] Bitcoin is often called the first cryptocurrency,^{[20][21][22]} although prior systems existed.^[note 8] Bitcoin is more correctly described as the first decentralized digital currency.^{[18][25]} It is the largest of its kind in terms of total market value.^[26]

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.^[18] Besides being obtained by mining, bitcoins can be exchanged for other currencies,^[27] products, and services.^[28] Users can send and receive bitcoins for an optional transaction fee.^[29]

Bitcoin as a form of payment for products and services has grown,^[28] and merchants have had an incentive to accept it because fees were generally^[30] lower than the 2–3% typically imposed by credit card processors.^[31] Unlike credit cards, any fees are paid by the purchaser, not the vendor. The European Banking Authority^[32] and other sources^{[18]:11} have warned that bitcoin users are not protected by refund rights or chargebacks. Despite a large increase in the number of merchants accepting bitcoin, the cryptocurrency does not have much momentum in retail transactions.^[33]

The use of bitcoin by criminals has attracted the attention of financial regulators,^[34] legislative bodies,^[35] law enforcement,^[36] and media.^[37] Criminal activities are primarily centered around black markets and theft, though officials in countries such as the United States also recognize that bitcoin can provide legitimate financial services.^[38]

Bitcoin has drawn the support of a few politicians, notably U.S. Presidential candidate Rand Paul, who accepts donations in bitcoin.^[39]

1.1.1 Design

Block chain

Main article: Block chain (database)

The *block chain* is a public ledger that records bitcoin transactions. A novel solution accomplishes this without any trusted central authority: maintenance of the block chain is performed by a network of communicating nodes running bitcoin software.^[18] Transactions of the form *payer X sends Y bitcoins to payee Z* are broadcast to this network using readily available software applications. Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes.^{[9]:ch. 8} The block chain 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 block chain. Approximately six times per hour, a new group of accepted transactions, a block, is

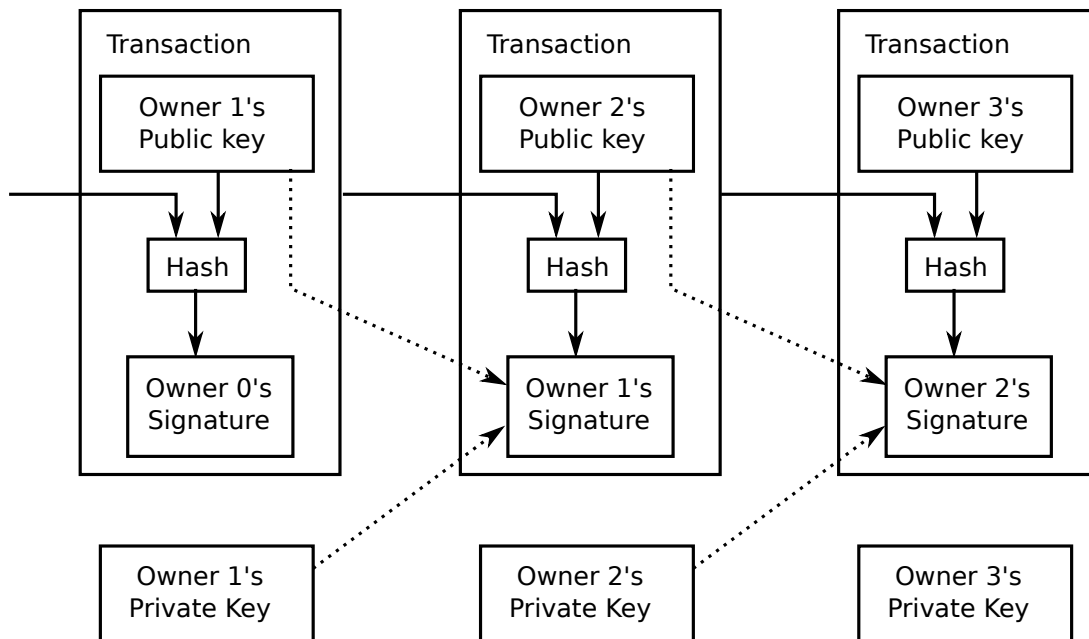
created, added to the block chain, and quickly published to all nodes. This allows bitcoin software to determine when a particular bitcoin amount has been spent, which is necessary in order to prevent **double-spending** in an environment without central oversight. Whereas a conventional ledger records the transfers of actual **bills** or **promissory notes** that exist apart from it, the block chain is the only place that bitcoins can be said to exist in the form of unspent outputs of transactions.^{[9]:ch. 5}

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][40]: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, which is one thousandth of bitcoin.^[41] One *microbitcoin* equals to 0.000001 bitcoin, which is one millionth of bitcoin. A microbitcoin is sometimes referred to as a *bit*.

On 7 October 2014, the **Bitcoin Foundation** disseminated a plan to apply for an ISO 4217 currency code for bitcoin,^[42] and mentioned BTC and XBT as the leading candidates.^[43]

Ownership



Simplified chain of ownership.^[11] 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**.^{[9]:ch. 5} If the private key is lost, the **bitcoin network** will not recognize any other evidence of ownership;^[18] 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 discarded a hard drive containing his private key.^[44]

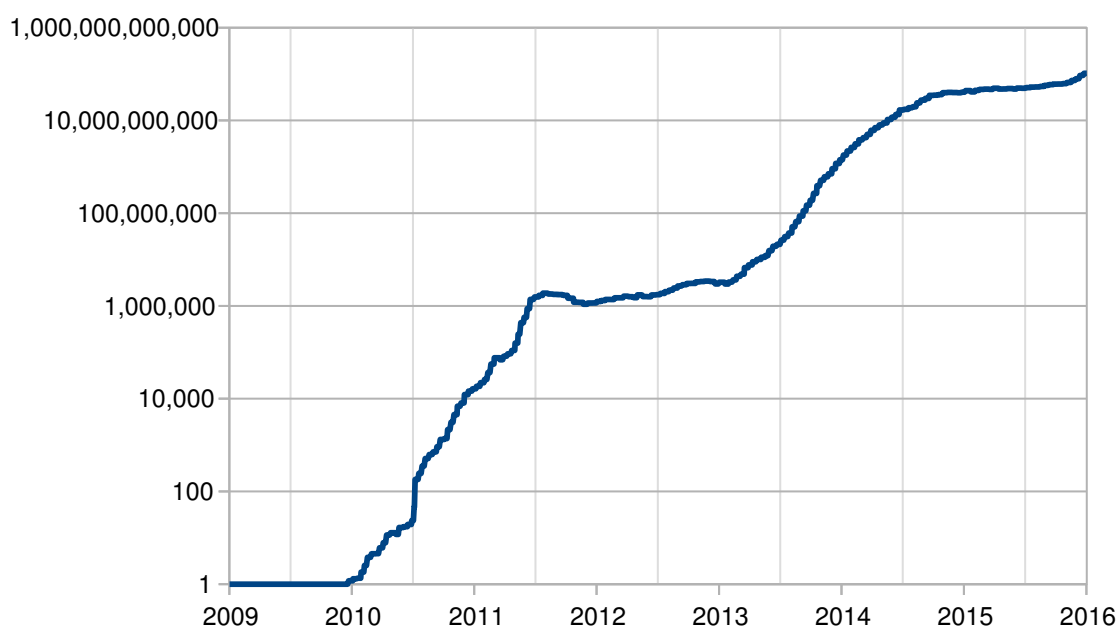
Transactions

See also: [Bitcoin network](#)

A transaction must have one or more inputs. 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 case, an additional output is used, returning the change back to the payer. Any input satoshis not accounted for in the transaction outputs become the transaction fee.^{[9]:ch. 5}

To send money to a bitcoin address, users can click links on webpages; this is accomplished with a provisional bitcoin URI scheme using a template registered with IANA. Bitcoin clients like Electrum and Armory support bitcoin URIs. Mobile clients recognize bitcoin URIs in QR codes, so that the user does not have to type the bitcoin address and amount in manually. The QR code is generated from the user input based on the payment amount. The QR code is displayed on the mobile device screen and can be scanned by a second mobile device.^[45]

Mining



Relative mining difficulty,^[note 9] the scale is logarithmic.^[46]

Mining is a record-keeping service.^[note 10] Miners keep the block chain consistent, complete, and unalterable by repeatedly verifying and collecting newly broadcast transactions into a new group of transactions called a *block*. A new block contains information that “chains” it to the previous block thus giving the block chain its name. It is a *cryptographic hash* of the previous block, using the *SHA-256* hashing algorithm.^{[9]:ch. 7}

In order to be accepted by the rest of the network, a new block must contain a so-called *proof-of-work*. 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*.^{[9]: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, ...^{[9]: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.^{[9]:ch. 8} For example, 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.^[48]

The proof-of-work system, alongside the chaining of blocks, makes modifications of the block chain extremely hard as an attacker must modify all subsequent blocks in order for the modifications of one block to be accepted. As



A mining farm in Iceland

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 organized *mining pools*,^[50] 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,^[51] although a fee may be charged for the service.^{[52][53]}

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.^[54] 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,^[55] even if they are a member of a pool.^[55]

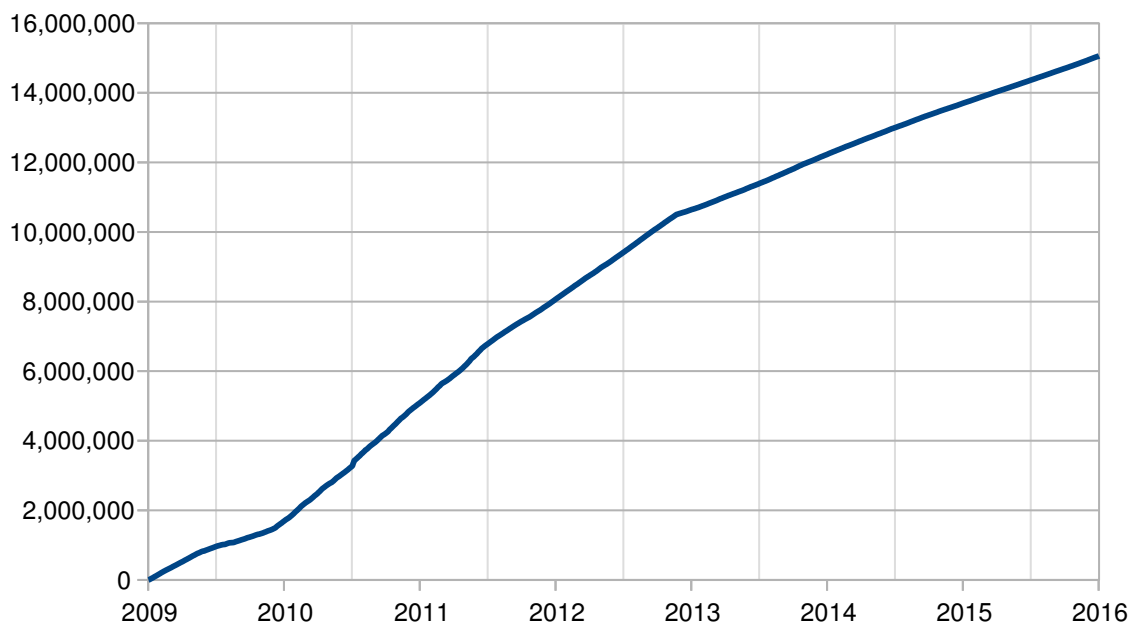
As of 2015, even if all miners used energy efficient processors, the combined electricity consumption would be 1.46 terawatt-hours per year—equal to the consumption of about 135,000 American homes.^[56] In 2013, electricity use was estimated to be 0.36 terawatt-hours per year or the equivalent of powering 31,000 US homes.^[57]

Supply

The successful miner finding the new block is rewarded with newly created bitcoins and transaction fees.^[58] As of 28 November 2012,^[59] the reward amounted to 25 newly created bitcoins per block added to the block chain. To claim the reward, a special transaction called a *coinbase* is included with the processed payments.^{[9]:ch. 8} All bitcoins in circulation can be traced back to such coinbase transactions. The bitcoin protocol specifies that the reward for adding a block will be halved approximately every four years. Eventually, the reward will decrease to zero, and the limit of 21 million bitcoins^[note 11] will be reached c. 2140; the record keeping will then be rewarded by transaction fees solely.^[60]

Transaction fees

Paying a transaction fee is optional, but may speed up confirmation of the transaction.^[61] Payers have an incentive to include such fees because doing so means their transaction is more likely to be added to the block chain sooner; miners can choose which transactions to process^[29] 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.^[62]

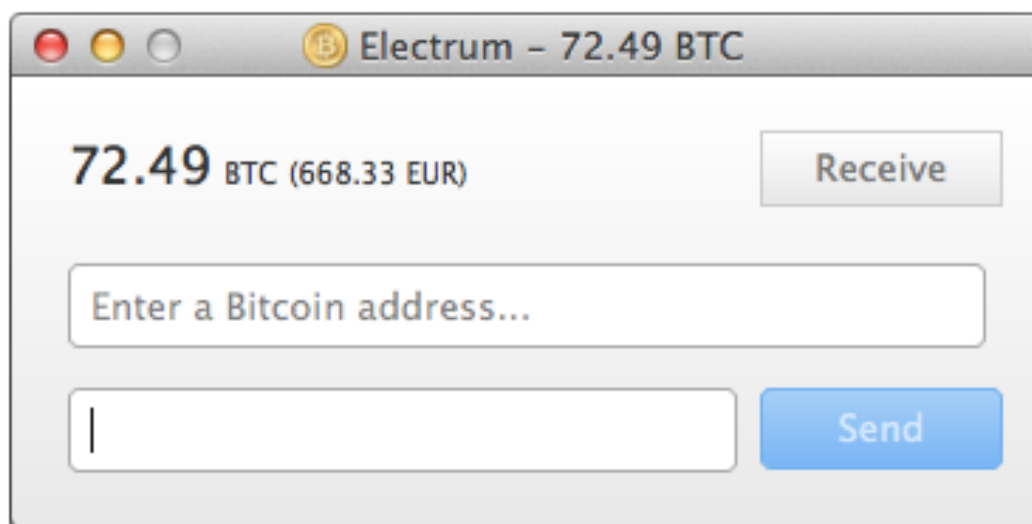


Total bitcoins in circulation.^[46]

Wallets

See also: [Digital wallet](#)

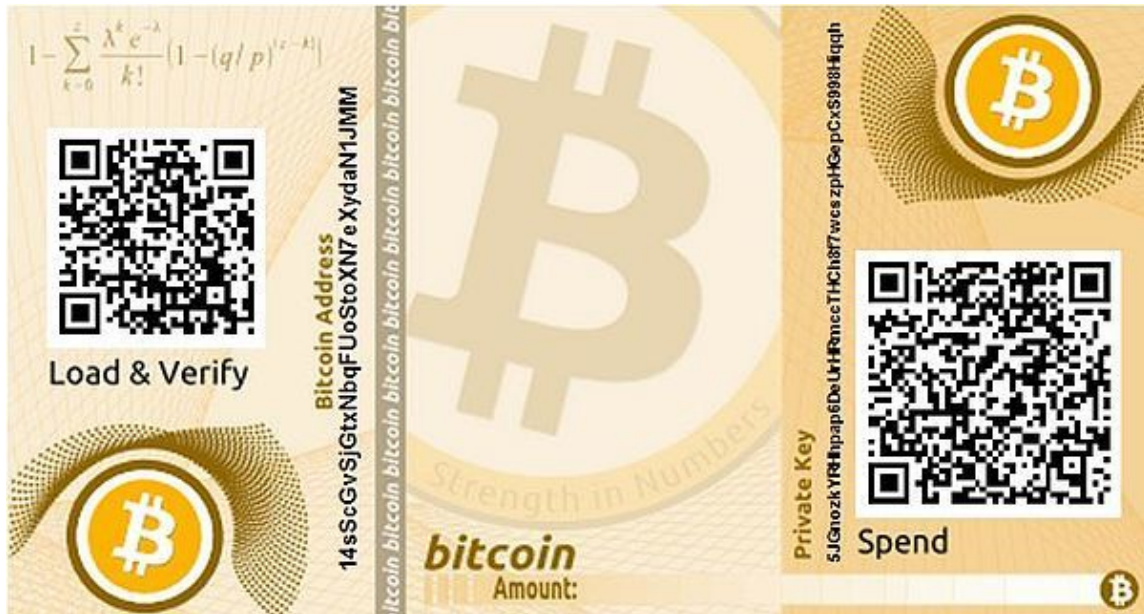
A *wallet* stores the information necessary to transact bitcoins. While wallets are often described as a place to hold^[63]



Electrum bitcoin wallet

or store bitcoins,^[64] due to the nature of the system, bitcoins are inseparable from the block chain transaction ledger. Perhaps a better way to describe a wallet is something that “stores the digital credentials for your bitcoin holdings”^[64] 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.^[65] 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.^[66] Software wallets can be split further in two categories: full clients and lightweight clients. Full clients find transactions directly on the block chain (over 60GB in 2016^[67]) and keeps



Bitcoin paper wallet generated at bitaddress.org



Trezor hardware wallet

growing, which may be an inconvenience for some users). Lightweight clients on the other hand consult a server to parse the block chain, and get only relevant transactions from the server (transactions to and from the user). When working with lightweight wallets, the user has to trust the server to a certain degree. The server can't steal bitcoins directly, or intercept transactions, but the server 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.

Next to software wallets, there are also internet services called *online wallets*, like Blockchain.info, Circle, Coinbase or CoinCorner. They offer similar functionality but may be easier to use. In these wallets, bitcoin credentials are stored with the online wallet provider rather than on the user's hardware.^{[68][69]} As a result, the user needs to have complete trust in the wallet provider. A malicious provider or a breach in server security may cause all bitcoins to be stolen.

Physical wallets also exist and are more secure, as they store the credentials necessary to spend bitcoins offline.^[64]

Examples combine a novelty coin with these credentials printed on metal,^{[70][71]} wood, or plastic. Others are simply paper printouts. Another type of wallet called a *hardware wallet* keeps credentials offline while facilitating transactions.^[72]

Reference implementation The first wallet program was released in 2009 by Satoshi Nakamoto as open-source code and was originally called *bitcoind*.^[73] 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.^[66] 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*.^[66] After the release of version 0.9, *Bitcoin-Qt* was renamed *Bitcoin Core*.^[74]

Privacy

Privacy is achieved by not identifying owners of bitcoin addresses while making other transaction data public. Bitcoin users are not identified by name, but transactions can be linked to individuals and companies.^[75] Additionally, bitcoin exchanges, where people buy and sell bitcoins for fiat money, may be required by law to collect personal information.^[76] To maintain financial privacy, a different bitcoin address for each transaction is recommended.^[77] Transactions that spend coins from multiple inputs can reveal that the inputs may have a common owner. Users concerned about privacy can use so-called mixing services that swap coins they own for coins with different transaction histories.^[78] It has been suggested that bitcoin payments should not be considered more private than credit card payments.^[79]

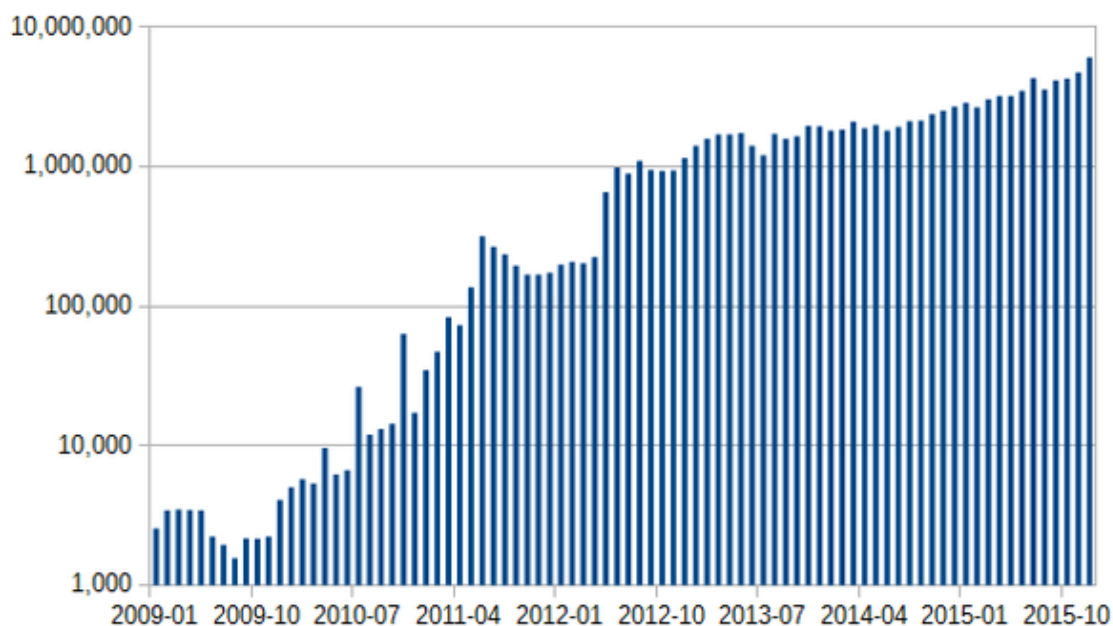
Fungibility

Wallets and similar software technically handle 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 block chain ledger, and that some users may refuse to accept bitcoins coming from controversial transactions, which would harm bitcoin’s fungibility.^[80] Projects such as *Zerocoin* and *Dark Wallet* aim to address these privacy and fungibility issues.^{[81][82]}

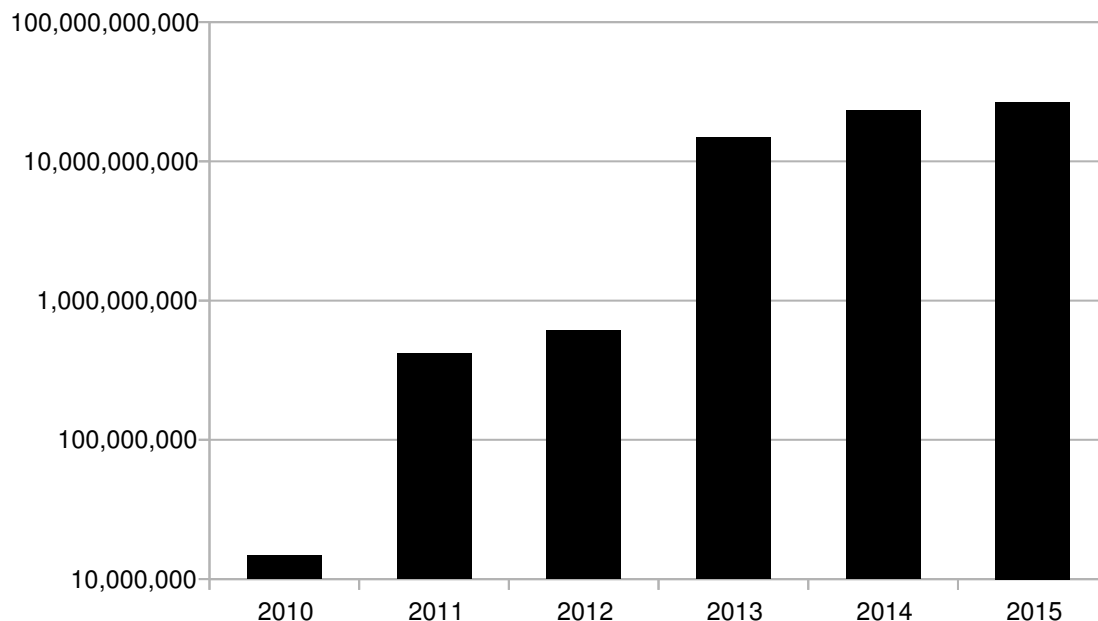
1.1.2 History

Main article: [History of bitcoin](#)

Bitcoin was invented by Satoshi Nakamoto,^[note 7] who published the invention on 31 October 2008 in a research paper



Number of bitcoin transactions per month (logarithmic scale).^[46]



Liquidity (estimated, USD/year, logarithmic scale).^[46]

called “Bitcoin: A Peer-to-Peer Electronic Cash System”.^[111] It was implemented as open source code and released in January 2009. Bitcoin is often called the first cryptocurrency^{[20][21][22]} although prior systems existed.^[note 8] Bitcoin is more correctly described as the first decentralized digital currency.^{[18][25]}

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.^{[83][84]}

Other early supporters were Wei Dai, creator of bitcoin predecessor *b-money*, and Nick Szabo, creator of bitcoin predecessor *bit gold*.^[85]

In 2010, an exploit in an early bitcoin client was found that allowed large numbers of bitcoins to be created.^[86] The artificially created bitcoins were removed when another chain overtook the bad chain.^[87]

Based on bitcoin’s open source code, other cryptocurrencies started to emerge in 2011.^[26]

In March 2013, a technical glitch caused a fork in the block chain, 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.^[88] Normal operation was restored when the majority of the network downgraded to version 0.7 of the bitcoin software.^[88]

In 2013 some mainstream websites began accepting bitcoins. WordPress had started in November 2012,^[89] followed by OKCupid in April 2013,^[90] TigerDirect^[91] and Overstock.com in January 2014,^[92] Expedia in June 2014,^[93] Newegg and Dell in July 2014,^[94] and Microsoft in December 2014.^{[95][note 12]} The Electronic Frontier Foundation, a non-profit group, started accepting bitcoins in January 2011,^[97] stopped accepting them in June 2011,^[98] and began again in May 2013.^[99]

In May 2013, the Department of Homeland Security seized assets belonging to the Mt. Gox exchange.^[100] The U.S. Federal Bureau of Investigation (FBI) shut down the Silk Road website in October 2013.^[101]

In October 2013, Chinese internet giant Baidu had allowed clients of website security services to pay with bitcoins.^[102] 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.^[103] 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.^[104] On the same day, one bitcoin traded for over RMB¥6780 (US\$1,100) in China.^[105] On 5 December 2013, the People’s Bank of China prohibited Chinese financial institutions from using bitcoins.^[106] After the announcement, the value of bitcoins dropped,^[107] and Baidu no longer accepted bitcoins for certain services.^[108] Buying real-world goods with any virtual currency has

been illegal in China since at least 2009.^[109]

The first bitcoin ATM was installed in October 2013 in Vancouver, British Columbia, Canada.^[110]

With about 12 million existing bitcoins in November 2013,^[111] the new price increased the market cap for bitcoin to at least US\$7.2 billion.^[112] By 23 November 2013, the total market capitalization of bitcoin exceeded US\$10 billion for the first time.^[113]

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.^[114]

In early February 2014, one of the largest bitcoin exchanges, Mt. Gox,^[115] suspended withdrawals citing technical issues.^[116] By the end of the month, Mt. Gox had filed for bankruptcy protection in Japan amid reports that 744,000 bitcoins had been stolen.^[117] Originally a site for trading Magic: The Gathering cards,^[118] Mt. Gox had once been the dominant bitcoin exchange but its popularity had waned as users experienced difficulties withdrawing funds.^[119]

On June 18, 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.^[120]

Less than one year after the collapse of Mt. Gox, United Kingdom-based exchange 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.^[121] The exchange remained offline for several days amid speculation that customers had lost their funds. Bitstamp resumed trading on January 9 after increasing security measures and assuring customers that their account balances would not be impacted.^[122]

The bitcoin exchange service Coinbase launched the first regulated bitcoin exchange in 25 US states on January 26, 2015. At the time of the announcement, CEO Brian Armstrong stated that Coinbase intends to expand to thirty countries by the end of 2015.^[123] 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.^[124]

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.^[125]

1.1.3 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”.^[126] Bitcoin is commonly referred to with terms like: digital currency,^{[18]:1} digital cash,^[127] virtual currency,^[4] electronic currency,^[12] or cryptocurrency.^[126] Its inventor, Satoshi Nakamoto, used the term electronic cash.^[11] 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”.^[128] 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.^[129] It does best as a medium of exchange.^[note 13] The bitcoin market currently suffers 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.^[129]

Journalists and academics also dispute what to call bitcoin. Some media outlets do make a distinction between “real” money and bitcoins,^[131] while others call bitcoin real money.^[132] *The Wall Street Journal* declared it a commodity in December 2013.^[133] A *Forbes* journalist referred to it as digital collectible.^[134] Two University of Amsterdam computer scientists proposed the term “money-like informational commodity”.^[135] In addition to that, *The Wall Street Journal*,^[15] *Wired*,^[136] *Daily Mail Australia*,^[137] *Forbes*,^[138] and *Business Wire*^[139] used the digital asset classification for bitcoin.

In the 21 September 2015 press release,^[140] the US Commodity Futures Trading Commission (CFTC) declared bitcoin to be a commodity covered by the Commodity Exchange Act.

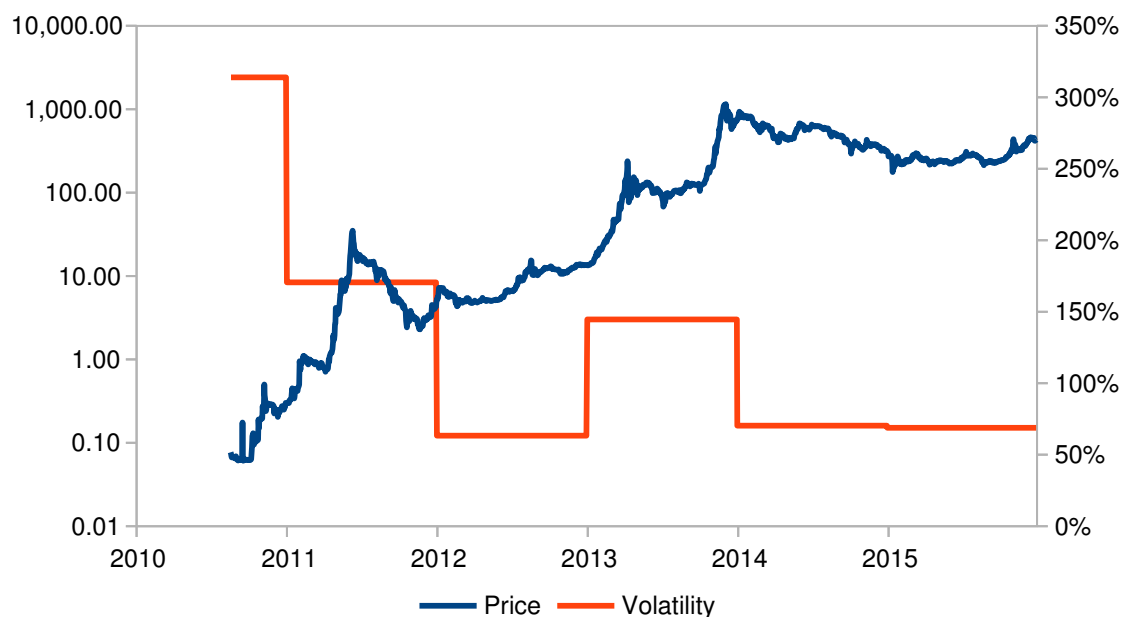
The People's Bank of China has stated that bitcoin “is fundamentally not a currency but an investment target”.^[141]

Buying and selling

A Bitcoin ATM in California.

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.^[142] Exchanges have since implemented measures to provide proof of reserves in an effort to convey transparency to users.^{[143][144]} Offline, bitcoins may be purchased directly from an individual^[145] or at a bitcoin ATM.^[146]

Price and volatility



Price^[note 14] (left vertical axis, logarithmic scale) and volatility^[note 15] (right vertical axis).^[46]

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.^[147]

Attempting to explain the high volatility, a group of Japanese scholars stated that there is no stabilization mechanism.^[148] The Bitcoin Foundation contends that high volatility is due to insufficient liquidity,^[149] while a *Forbes* journalist claims that it is related to the uncertainty of its long-term value,^[150] 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.”^[151]

There are uses where volatility does not matter, such as online gambling, tipping, and international remittances.^[151] 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.^[152]

The price of bitcoins has gone through various cycles of appreciation and depreciation referred to by some as bubbles and busts.^{[153][154]} In 2011, the value of one bitcoin rapidly rose from about US\$0.30 to US\$32 before returning to US\$2.^[155] In the latter half of 2012 and during the 2012–13 Cypriot financial crisis, the bitcoin price began to rise,^[156] reaching a high of US\$266 on 10 April 2013, before crashing to around US\$50.^[157] On November 29, 2013, the cost of one bitcoin rose to the all-time peak of US\$1,242.^[158] 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.^[159] 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.”^[160] 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.^[161]

Speculative bubble dispute

Bitcoin has been labelled a *speculative bubble* by many including former Fed Chairman Alan Greenspan^[162] and economist John Quiggin.^[163] Nobel Memorial Prize laureate Robert Shiller said that bitcoin “exhibited many of the characteristics of a speculative bubble”.^[164] Two lead software developers of bitcoin, Gavin Andresen^[165] and Mike Hearn,^[166] 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.^{[47]: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.^[167] The *Washington Post* pointed out that the observed cycles of appreciation and depreciation don't correspond to the definition of speculative bubble.^[155]

Ponzi scheme dispute

Various journalists,^[168] U.S. economist Nouriel Roubini,^[169] and the head of the Estonian central bank^[170] have voiced concerns that bitcoin may be a Ponzi scheme. A 2012 report by the European Central Bank stated, "it [is not] easy to assess whether or not the bitcoin system actually works like a pyramid or Ponzi scheme."^{[171]:27} A 2014 report by the World Bank concluded that "contrary to a widely-held opinion, bitcoin is not a deliberate Ponzi".^{[172]:7} In the opinion of Eric Posner, a law professor at the University of Chicago, "A real Ponzi scheme takes fraud; bitcoin, by contrast, seems more like a collective delusion."^[168]

U.S. economist Nouriel Roubini, a former senior adviser to the U.S. Treasury and the International Monetary Fund, has stated that bitcoin is "a Ponzi game".^[173] In February 2014, an asset manager and columnist for *The New York Post* called bitcoin a Ponzi scheme, opining, "Welcome to 21st-century Ponzi scheme: Bitcoin".^[174] The head of the Estonian central bank, Mihkel Nommela, stated, "virtual currency schemes are an innovation that deserves some caution, given the lack of ... evidence that this isn't just a Ponzi scheme."^[170]

Others have expressed the opinion that bitcoin is not a Ponzi scheme. *The Huffington Post* asked, "is bitcoin a Ponzi scheme, yes or no?" and answered itself with a definitive "no!"^[175] *PC World* magazine stated, "bitcoin is clearly not a Ponzi scheme".^[176] Economist Jeffrey Tucker published an article by John Mather claiming that "there are several key differences between a Ponzi scheme and bitcoin."^[177] A 2014 report by the Swiss Federal Council states, "the question is repeatedly raised whether bitcoin can be deemed an impermissible pyramid scheme... since in the case of bitcoin the typical promises of profits are lacking, it cannot be assumed that bitcoin is a pyramid scheme."^{[178]: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".^[163] A similar forecast was made in November 2014 by economist Kevin Dowd.^[179] 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.^[180] In the indicated period bitcoin has exchanged as low as \$176.50 (January 2015) and during November 2015 the bitcoin low was \$309.90.^[46] In December 2013, teacher Mark T. Williams forecast a bitcoin would be worth less than \$10 by July 2014.^[181] In the indicated period bitcoin has exchanged as low as \$344 (April 2014) and during July 2014 the bitcoin low was \$609.^{[46][182]} In December 2014, Williams said, "The probability of success is low, but if it does hit, the reward will be very large."^[183] In May 2013, Bank of America FX and Rate Strategist David Woo forecast a maximum fair value per bitcoin of \$1,300.^[184] Bitcoin investor Cameron Winklevoss stated in December 2013 that the "small bull case scenario for bitcoin is... 40,000 USD a coin".^[185]

Obituaries

The "death" of bitcoin has been proclaimed numerous times.^[186] One journalist has recorded 29 such "obituaries" as of early 2015.^[186] *Forbes* magazine declared bitcoin "dead" in June 2011,^[187] followed by *Gizmodo Australia* in August 2011.^[188] *Wired* magazine wrote it had "expired" in December 2012,^[189] *Ouishare Magazine* declared, "game over, bitcoin" in May 2013,^[190] and *New York Magazine* stated bitcoin was "on its path to grave" in June 2013.^[191] *Reuters* published an "obituary" for bitcoin in January 2014.^[192] *Street Insider* declared bitcoin "dead" in February 2014,^[193] as did *The Weekly Standard* in March 2014,^[194] followed by *Salon* in March 2014,^[195] and *Vice News* in March 2014,^[196] then the *Financial Times* in September 2014.^[197] In January 2015, *USA Today* states bitcoin was "headed to the ash heap",^[198] and *The Telegraph* declared "the end of bitcoin experiment".^[199] In January 2016, former bitcoin developer Mike Hearn called bitcoin a "failed project".^[200] 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".^[201]

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”.^[202] 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.^[203] Economist John Quiggin has criticized bitcoin as “the final refutation of the efficient-market hypothesis”.^[163]

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.^{[47]:33[204][205]}

Free software movement activist Richard Stallman has criticized the lack of anonymity and called for reformed development.^[206] 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.^[207] 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.”^[208]

Similarly, Peter Schiff, a bitcoin sceptic understands “the value of the technology as a payment platform” and his Euro Pacific Precious Metals fund partnered with BitPay in May 2014, because “a wire transfer of fiat funds can be slow and expensive for the customer”.^[209]

Officials in countries such as Brazil,^[210] the Isle of Man,^[211] Jersey,^[212] the United Kingdom,^[213] and the United States^[38] 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.^{[214][215][216]}

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.^[130] As of December 2014 established firms that accept payments in bitcoin include Clearly Canadian,^[217] Dell,^[218] Dish Network,^[219] Dynamite Entertain-

ment,^[220] Expedia,^[221] Microsoft,^[95] Newegg,^[222] PrivateFly,^[223] Overstock.com,^[92] the Sacramento Kings,^[224] TigerDirect,^[91] Time Inc.,^[225] Virgin Galactic,^[226] and Zynga.^{[227][note 12]} Due to the fact that chargebacks are impossible, retailers usually offer in-store credit as the only option when returning items purchased with bitcoins.^[228] As of September 2014 PayPal allows North American merchants using its system the ability to receive payment in bitcoins.^[229]

Acceptance by nonprofits

Organizations accepting donations in bitcoin include: The Electronic Frontier Foundation,^[99] Greenpeace,^[230] The Mozilla Foundation,^[231] and The Wikimedia Foundation.^[232] Some U.S. political candidates, including New York City Democratic Congressional candidate Jeff Kurzon have said they would accept campaign donations in bitcoin.^[233] In late 2013 the University of Nicosia became the first university in the world to accept bitcoins.^[234]

Use in retail transactions

Due to the design of bitcoin, all retail figures are only estimates.^{[33][235]} 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.^[235] 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,^[33] and concluded that in 2014 “it appears there has been very little if any increase in retail purchases using bitcoin.”^[33]

Financial institutions

Bitcoin companies have had difficulty opening traditional bank accounts because lenders have been leery of bitcoin’s links to illicit activity.^[236] According to Antonio Gallippi, a co-founder of BitPay, “banks are scared to deal with bitcoin companies, even if they really want to”.^[237] In 2014, the National Australia Bank closed accounts of businesses with ties to bitcoin,^[238] and HSBC refused to serve a hedge fund with links to bitcoin.^[239]

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.”^[240] In June 2014, the first bank that converts deposits in currencies instantly to bitcoin without any fees was opened in Boston.^[241]

As an investment

Some Argentinians have bought bitcoins to protect their savings against high inflation or the possibility that governments could confiscate savings accounts.^[76] During the 2012–2013 Cypriot financial crisis, bitcoin purchases in Cyprus rose due to fears that savings accounts would be confiscated or taxed.^[242] 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.^[243] 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^[244]) to establish a bitcoin ETF.^[245] As of early 2015, they have announced plans to launch a New York-based bitcoin exchange named Gemini,^[246] which has received approval to launch on 5 October 2015.^[247] On 4 May 2015, Bitcoin Investment Trust started trading on the OTCQX market as GBTC.^[248] Forbes started publishing arguments in favor of investing in December 2015.^[249]

In 2013 and 2014, the European Banking Authority^[32] and the Financial Industry Regulatory Authority (FINRA), a United States self-regulatory organization,^[250] warned that investing in bitcoins carries significant risks. Forbes named bitcoin the best investment of 2013.^[251] In 2014, Bloomberg named bitcoin one of its worst investments of the year.^[252] In 2015, bitcoin topped Bloomberg’s currency tables.^[253]

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.^{[152][254]} 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.^[255]

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.^[256] 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,^[257] at the time called 'mystery buyer'.^[258] The company's goal is to fund 100 bitcoin businesses within 2–3 years with \$10,000 to \$20,000 for a 6% stake.^[257] Investors also invest in bitcoin mining.^[259]

Political economy

The decentralization of money offered by virtual currencies like bitcoin has its theoretical roots in the Austrian school of economics,^[260] 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.^[261]

Bitcoin appeals to tech-savvy libertarians, because it so far exists outside the institutional banking system and the control of governments.^[262] 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.^[263]

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”^[264] and socialists proposing their “own states, complete with currencies”,^[265] 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,^[266] “because governments are not fully living up to the responsibility that comes with state-sponsored money”.^[267] 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”.^[268] Two WSJ journalists describe bitcoin in their book as “about freeing people from the tyranny of centralised trust”.^[269]

1.1.4 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.

In April 2013, Steven Strauss, a Harvard public policy professor, suggested that governments could outlaw bitcoin,^[270] and this possibility was mentioned again by a bitcoin investment vehicle in a July 2013 report to a regulator.^[245] However, the vast majority of nations have not done so as of 2014. It is illegal in Bangladesh,^[271] Bolivia,^[272] Ecuador^[273] and Russia.^[274]

1.1.5 Criminal activity

The use of bitcoin by criminals has attracted the attention of financial regulators, legislative bodies, law enforcement, and the media.^[34] The FBI prepared an intelligence assessment,^[36] the SEC has issued a pointed warning about investment schemes using virtual currencies,^[34] and the U.S. Senate held a hearing on virtual currencies in November 2013. CNN has referred to bitcoin as a “shady online currency [that is] starting to gain legitimacy in certain parts of the world”,^[275] and *The Washington Post* called it “the currency of choice for seedy online activities”.^[37]

Several news outlets have asserted that the popularity of bitcoins hinges on the ability to use them to purchase illegal goods.^{[276][277]} 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.”^[263]

Theft

There have been many cases of bitcoin theft.^[65] One way this is accomplished involves a third party accessing the private key to a victim's bitcoin address,^[278] or of an online wallet.^[279] 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.^[245]

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.^[280] Users tracked the coins as they were processed and converted to cash, but no funds were recovered and no culprits identified.^[280] 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.^[281]

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.^[282] 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.^[117] *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.^[283] *Poloniex*, a digital currency exchange, reported on March 2014 that it lost bitcoins valued at around \$50,000.^[284] In January 2015 UK-based *bitstamp*, the third busiest bitcoin exchange globally, was hacked and \$5 million in bitcoins were stolen.^[285] February 2015 saw a Chinese exchange named *BTER* lose bitcoins worth nearly \$2 million to hackers.^[286]

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*.^[287] Child pornography,^[288] murder-for-hire services,^[289] and weapons^[290] 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.^[291]

Several deep web black markets have been shut by authorities. In October 2013 *Silk Road* was shut down by U.S. law enforcement^{[292][293][294]} leading to a short-term decrease in the value of bitcoin.^[295] In 2015, the founder of the site was sentenced to life in prison.^[296] 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.^[297] In early 2014, Dutch authorities closed *Utopia*, an online illegal goods market, and seized 900 bitcoins.^[298] 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*.^[299] 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,^[300] and in February, 2015, its founder, *Ross Ulbricht*, was convicted on drugs charges and faces a life sentence.^[301]

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.^[302] In a separate case, escrow accounts with bitcoins belonging to patrons of a different black market were hacked in early 2014.^[281]

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.^[288] Some of these sites have shut down, such as a deep web crowdfunding website that aimed to fund the creation of new child porn.^[303] Furthermore, hyperlinks to child porn websites have been added to the block chain as arbitrary data can be included when a transaction is made.^{[304][305]}

Money laundering

Bitcoins may not be ideal for money laundering because all transactions are public.^[306] Authorities, including the *European Banking Authority*^[32] the *FBI*,^[36] and the *Financial Action Task Force* of the *G7*^[307] 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.^[114]

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.^[308] 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”.^[308] In September 2014 the judge fined Bitcoin Savings & Trust and its owner \$40 million for operating a bitcoin Ponzi scheme.^[309]

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.^[310]

Unauthorized mining In June 2011, Symantec warned about the possibility that botnets could mine covertly for bitcoins.^[311] Malware used the parallel processing capabilities of GPUs built into many modern video cards.^[312] 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.^[313]

In mid-August 2011, bitcoin mining botnets were detected,^[314] and less than three months later, bitcoin mining trojans had infected Mac OS X.^[315]

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.^[316]

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.^[317]

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.^[318] 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.^[319]

Several reports of employees or students using university or research computers to mine bitcoins have been published.^[320]

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.^[321] Many of these also log keystrokes to record passwords, often avoiding the need to crack the keys.^[321] 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.^[322] 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.^[323] Security company Trustwave, which tracked the malware, reports that its latest version was able to steal 30 types of digital currency.^[324]

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.^[325] A different trojan for Mac OS X, called CoinThief was reported in February 2014 to be responsible for multiple bitcoin thefts.^[325] The software was hidden in versions of some cryptocurrency apps on Download.com and MacUpdate.^[325]

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.^[326] 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.^[327] 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.^[326]

1.1.6 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 block chain.^[49] Other attacks, such as theft of private keys, require due care by users.

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.^[18]

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 block chain) that is visible to all users, and ensuring for all transferred bitcoins that they haven't been previously spent.^{[18]: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 block chain.^[328]

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 block chain.^[329]

History modification

The other principal way to steal bitcoins would be to modify block chain ledger entries.

For example, Eve could buy something from Alice, like a sofa, by adding a signed entry to the block chain ledger equivalent to *Eve pays Alice 100 bitcoins*. Later, after receiving the sofa, Eve could modify that block chain ledger entry to read instead: *Eve pays Alice 1 bitcoin*, or replace Alice's address by another of Eve's addresses. Digital signatures cannot prevent this attack: Eve can simply sign her entry again after modifying it.

To prevent modification attacks, each block of transactions that is added to the block chain includes a **cryptographic hash code** that is computed from the hash of the previous block as well as all the information in the block itself. When the bitcoin software notices two competing block chains, it will automatically assume that the chain with the greatest amount of work to produce it is the valid one. Therefore, in order to modify an already recorded transaction (as in the above example), the attacker would have to recalculate not just the modified block, but all the blocks after the modified one, until the modified chain contains more work than the legitimate chain that the rest of the network has been building in the meantime. Consequently, for this attack to succeed, the attacker must outperform the honest part of the network.^[49]

Each block that is added to the block chain, 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 block chain—unless the attacker controls more than half the total network power, in which case it is called a 51% attack.^[330] For example, if the attacker possesses 10% of the calculation power of the bitcoin network and the shop requires 6 confirmations for a successful transaction, the probability of success of such an attack will be 0.02428%.^[11]

Selfish mining

This attack was first introduced by Ittay Eyal and Emin Gun Sirer at the beginning of November 2013.^[331] In this attack, the attacker finds blocks but does not broadcast them. Instead, the attacker mines their own private chain and eventually (when another miner or network of miners finds their own block) publishes several private blocks in a row. This forces the “honest” network to abandon their previous work and switch to the attacker’s branch. As a result, honest miners lose a significant part of their revenue, while the attacker increases their profits due to changes in relative hashpowers.

According to the authors, a rational miner observing a selfish mining attacker would have an incentive to join the attacker’s pool, thereby increasing the attacker’s hashpower. This makes the attack and incentives even stronger, thus potentially leading to a 51% attack and the collapse of the currency.

Gavin Andresen and Ed Felten disagreed with this conclusion,^[332] Felten defending his assertion that the bitcoin protocol is incentive compatible.^[29] The original authors responded that the disagreement stemmed from Felten’s misunderstanding of how miners are compensated in mining pools,^[333] that the assertion was in error, given the presence of a strategy that dominates honest mining, and that the error stemmed from Felten et al. not modeling block withholding attacks in their analysis.^[334]

Deanonymisation of clients

Along with transaction graph analysis, which may reveal connections between bitcoin addresses (pseudonyms),^{[2][335]} there is a possible attack^[336] which links a user’s pseudonym to its IP address, even if the peer is using Tor. 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.^[336]

1.1.7 Alternative applications of the block chain

In January 2015 IBM’s Institute for Business Value announced a concept called ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) where network-connected devices can interact autonomously on the Internet of things using freely available technology including bittorrent, Telehash, and bitcoin.^[337] This is not an IBM product^[337] but instead a concept system.^[338] IBM has also explored using the block chain as part of a payment system that would allow transactions in major currencies.^[339]

In May 2015 NASDAQ OMX Group announced a pilot study using bitcoins of negligible value, called “colored coins”, to represent and transfer pre-IPO trading shares on its Nasdaq Private Markets.^{[340][341]} In the same month the government of Honduras announced plans to use Bitcoin technology to host a land title registry.^[342]

1.1.8 Data in the block chain

While it is possible to store any digital file in the block chain, the larger the transaction size, the larger any associated fees become.^[62] 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.^[343]

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.^{[344][345]} Similar initiatives have been created by students and groups at other universities, such as Stanford University and the University of California, Berkeley.

1.1.10 In art, entertainment, and media

Fine arts

The Museum of Applied Arts, Vienna purchased a work by Dutch artist Harm van den Dorpel in 2015 and became the first museum to acquire art work using bitcoin.^[346]

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.^[347]

In the film *Dope* a group of three friends organize an online network through bitcoin transactions that would allow them to sell drugs without getting it traced back to them.

Music

Several lighthearted songs celebrating bitcoin have been released.^[348]

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.^[349]

Radio

On April 25, 2013, the weekly Mexican Public Radio technology program, *1060 Interfase* produced by Radio Educación, broadcast two shows dedicated to bitcoin.^{[350][351]}

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.^[352]
- In Season 3, the CBS show *The Good Wife* featured an episode alluding to the creator of bitcoin as well as the FBI investigating the case. The episode titled 'Bitcoin for Dummies' was shown in early 2012.^[353]
- The CBS series *CSI: Cyber* featured an episode about bitcoin during its first season, entitled "Bit by Bit". The plot focused on the theft of bitcoins from a small family-run business.
- In November 2015, on the reality television show *Judge Judy* a bitcoin trader lost a case where he had claimed to be involved in an elaborate man-in-the-middle scheme.^[354]

1.1.11 Bibliography

- Paul Vigna, Michael Casey (January 27, 2015). *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. St. Martin's Press. ISBN 1250065631.
- Nathaniel Popper (May 19, 2015). *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. HarperCollins Publishers. ISBN 978-0062362490.
- Andreas Antonopoulos (December 3, 2014). *Mastering Bitcoin*. O'Reilly Media. ISBN 978-1449374044.

1.1.12 See also

- Alternative currency
- Digital gold currency
- Bitcoin XT
- Bitcoin Classic
- Crypto-anarchism
- Decentralized autonomous organization
- Electronic money
- Private currency
- Proof-of-work system
- World currency

1.1.13 Notes

- [1] Bitcoin does not have a central authority.^[1] Date of introduction 3 January 2009 User(s) Worldwide Supply growth 25 bitcoins per block (approximately every ten minutes) until mid 2016,^[2] and then afterwards 12.5 bitcoins per block for 4 years until next halving. This halving continues until 2110–40, when 21 million bitcoins 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]
- [5] The word *bitcoin* is a compound of the words *bit* and *coin*.^[10] The white paper that defined bitcoin^[11] frequently uses the shorter *coin*.
- [6] 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.^[12] The WSJ^[13] and The Chronicle of Higher Education^[14] advocate use of lowercase *bitcoin* in all cases. This article follows the latter convention.
- [7] It is not known whether the name *Satoshi Nakamoto* is real or a pseudonym, or if it represents one person or a group.^[16]
- [8] DigiCash was first used for a transaction in 1994,^[23] and OpenCoin, now known as Ripple, had code written prior to November 2008.^[24]
- [9] Relative mining difficulty is defined as the ratio of the difficulty target on 9 January 2009 to the current difficulty target.
- [10] 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.^[47]
- [11] The exact number is 20999999.9769 bitcoins.^{[9]:ch. 8}
- [12] Some of these firms use bitcoin payment processors such as BitPay and Coinbase and do not handle or store bitcoins themselves.^[96]
- [13] As of 2015 the number of merchants accepting bitcoin has passed 100,000.^[130]
- [14] The price of 1 bitcoin in U.S. dollars.
- [15] Volatility is calculated on a yearly basis.

1.1.14 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] Andreas M. Antonopoulos (April 2014). *Mastering Bitcoin. Unlocking Digital Crypto-Currencies*. O'Reilly Media. Retrieved 23 October 2014.
- [10] “bitcoin”. Oxford University Press. Retrieved 28 December 2014.
- [11] Nakamoto, Satoshi (October 2008). “Bitcoin: A Peer-to-Peer Electronic Cash System” (PDF). *bitcoin.org*. Retrieved 28 April 2014.
- [12] 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.
- [13] Vigna, Paul (3 March 2014). “BitBeat: Is It Bitcoin, or bitcoin? The Orthography of the Cryptography”. *WSJ*. Retrieved 21 April 2014.
- [14] Metcalf, Allan (14 April 2014). “The latest style”. *Lingua Franca blog*. The Chronicle of Higher Education (*chronicle.com*). Retrieved 19 April 2014.
- [15] 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.
- [16] S., L. (2 November 2015). “Who is Satoshi Nakamoto?”. *The Economist explains* (The Economist). Retrieved 11 December 2015.
- [17] Davis, Joshua (10 October 2011). “The Crypto-Currency: Bitcoin and its mysterious inventor”. *The New Yorker*. Retrieved 31 October 2014.
- [18] Jerry Brito and Andrea Castillo (2013). “Bitcoin: A Primer for Policymakers” (PDF). *Mercatus Center*. George Mason University. Retrieved 22 October 2013.
- [19] 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 “block chain”
- [20] “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.
- [21] Sparkes, Matthew (9 June 2014). “The coming digital anarchy”. *The Telegraph* (London: Telegraph Media Group Limited). Retrieved 7 January 2015.
- [22] 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.

- [23] “World’s first electronic cash payment over computer networks.”. Electronic Frontier Foundation. 26 May 1994. Retrieved 20 November 2015.
- [24] “OpenCoin/opencoin-historic”. *github.com*. GitHub, Inc. Retrieved 8 May 2015.
- [25] Sagona-Stopfel, Katherine. “Bitcoin 101 white paper” (PDF). Thomson Reuters. Retrieved 20 November 2015.
- [26] 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 3 November 2014.
- [27] “What is Bitcoin?”. CNN Money. Retrieved 16 November 2015.
- [28] Natasha Lomas (16 September 2013). “BitPay Passes 10,000 Bitcoin-Accepting Merchants On Its Payment Processing Network”. *Techcrunch*. Techcrunch.com. Retrieved 21 October 2013.
- [29] 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 8 May 2014. A transaction fee is like a tip or gratuity left for the miner.
- [30] Hearn, Mike (15 January 2016). “The resolution of the Bitcoin experiment”. *Medium.com*. Retrieved 15 January 2016.
- [31] Wingfield, Nick (30 October 2013). “Bitcoin Pursues the Mainstream”. *The New York Times*. Retrieved 4 November 2013.
- [32] “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.
- [33] Orcutt, Mike (18 February 2015). “Is Bitcoin Stalling?”. *MIT Technology Review*. Retrieved 20 Feb 2015.
- [34] Lavin, Tim (8 August 2013). “The SEC Shows Why Bitcoin Is Doomed”. *bloomberg.com* (Bloomberg LP). Retrieved 20 October 2013.
- [35] Tracy, Ryan (Nov 5, 2013). “Bitcoin Comes Under Senate Scrutiny”. *Washington Wire*. Wall Street Journal. Retrieved 20 December 2014.
- [36] “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.
- [37] Timothy B. Lee and 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.
- [38] Tracy, Ryan (18 November 2013). “Authorities See Worth of Bitcoin”. *Markets* (The Wall Street Journal). Retrieved 28 November 2014.
- [39] Higgins, Stan (7 April 2015). “Rand Paul Accepts Bitcoin for Presidential Campaign”. CoinDesk. Retrieved 23 October 2015.
- [40] “Regulation of Bitcoin in Selected Jurisdictions” (PDF). The Law Library of Congress, Global Legal Research Center. January 2014. Retrieved 26 August 2014.
- [41] Katie Pisa and Natasha Maguder (9 July 2014). “Bitcoin your way to a double espresso”. *cnn.com* (CNN). Retrieved 23 April 2015.
- [42]
- [43] “Press Release October 7, 2014: Bitcoin Foundation Financial Standards Working Group Leads the Way for Mainstream Bitcoin Adoption”. *Press Release*. Bitcoin Foundation. 7 October 2014. Retrieved 7 November 2014.
- [44] “Man Throws Away 7,500 Bitcoins, Now Worth \$7.5 Million”. *CBS DC*. 29 November 2013. Retrieved 23 January 2014.
- [45] Don W. Tyler, Jeff Isenhardt, Anne Mueller, Christoph Sadil (8 May 2014). “Qr code-enabled p2p payment systems and methods.US 20140129428 A1” (Patent application). *uspto.gov*. Retrieved 20 January 2015.
- [46] “Charts”. *Blockchain.info*. Retrieved 2 November 2014.
- [47] 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.
- [48] “Difficulty History” (The ratio of all hashes over valid hashes is $D \times 4295032833$, where D is the published “Difficulty” figure.). *Blockchain.info*. Retrieved 26 March 2015.

- [49] Ramzan, Zufikar (2014). "Bitcoin: What is it?". The Khan Academy. Retrieved 5 April 2014.
- [50] Mills, Kelly (3 April 2014). "Bitcoins lose viability". *The Arbitrator*. Boise State Student Media. Retrieved 14 April 2014.
- [51] Wang, Luqin; Liu, Yong. "Exploring Miner Evolution in Bitcoin Network" (PDF). NYU Polytechnic School of Engineering. Retrieved 15 February 2015.
- [52] Rosenfeld, Meni. "Analysis of Bitcoin Pooled Mining Reward Systems" (PDF). Retrieved 14 February 2015.
- [53] Peter Svensson (17 June 2014). "Bitcoin faces biggest threat yet: a miner takeover". Retrieved 8 January 2015.
- [54] Rockman, Simon (17 January 2014). "Manic miners: Ten Bitcoin generating machines". The Register. Retrieved 13 February 2014.
- [55] Bays, Jason (9 April 2014). "Bitcoin offers speedy currency, poses high risks". *Purdue Exponent*. The Exponent Online. Retrieved 14 April 2014.
- [56] "The magic of mining". *The economist*. 13 January 2015. Retrieved 13 January 2015.
- [57] Gimein, Mark (13 April 2013). "Virtual Bitcoin Mining Is a Real-World Environmental Disaster". *Bloomberg Business* (Bloomberg LP). Retrieved 22 April 2015.
- [58] Ashlee Vance (14 November 2013). "2014 Outlook: Bitcoin Mining Chips, a High-Tech Arms Race". *Businessweek*. Retrieved 24 November 2013.
- [59] "Block #210000". *Blockchain.info*. Retrieved 20 November 2015.
- [60] 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.
- [61] "How much will the transaction fee be?". *FAQ*. Bitcoin Foundation. Retrieved 19 March 2014.
- [62] "How much will the transaction fee be?". *Bitcoinfees.com*. Retrieved 30 November 2014.
- [63] Adam Serwer and Dana Liebelson (10 April 2013). "Bitcoin, Explained". *motherjones.com*. Mother Jones. Retrieved 26 April 2014.
- [64] Villaseñor, John (26 April 2014). "Secure Bitcoin Storage: A Q&A With Three Bitcoin Company CEOs". *forbes.com* (Forbes). Retrieved 26 April 2014.
- [65] "Bitcoin: Bitcoin under pressure". *The Economist*. 30 November 2013. Retrieved 30 November 2013.
- [66] Skudnov, Rostislav (2012). *Bitcoin Clients* (PDF) (Bachelor's Thesis). Turku University of Applied Sciences. Retrieved 16 January 2014.
- [67] "Information about cryptocurrency networks". Retrieved 2 January 2016.
- [68] Jon Matonis (26 April 2012). "Be Your Own Bank: Bitcoin Wallet for Apple". *Forbes*. Retrieved 17 November 2014.
- [69] Bill Barhydt (4 Jun 2014). "3 reasons Wall Street can't stay away from bitcoin". *NBCUniversal*. Retrieved 2 April 2015.
- [70] Staff, Verge (13 December 2013). "Casascius, maker of shiny physical bitcoins, shut down by Treasury Department". The Verge. Retrieved 10 January 2014.
- [71] Staff, Coindesk (13 April 2015). "Finnish Startup Launches 'Low-Cost' Physical Bitcoins". *Coindesk*. Retrieved 13 April 2015.
- [72] Eric Mu (15 October 2014). "Meet Trezor, A Bitcoin Safe That Fits Into Your Pocket". *Forbes Asia* (Forbes). Retrieved 31 October 2014.
- [73] "Bitcoin-Qt/bitcoind version 0.5.0". Retrieved 6 May 2015.
- [74] "Bitcoin Core version 0.9.0 released". *bitcoin.org*. Retrieved 8 January 2015.
- [75] Simonite, Tom (5 September 2013). "Mapping the Bitcoin Economy Could Reveal Users' Identities". *MIT Technology Review*. Retrieved 2 April 2014.
- [76] Lee, Timothy (21 August 2013). "Five surprising facts about Bitcoin". The Washington Post. Retrieved 2 April 2014.
- [77] McMillan, Robert (6 June 2013). "How Bitcoin lets you spy on careless companies". *wired.co.uk*. Conde Nast. Retrieved 2 April 2014.

- [78] Matonis, Jon (5 June 2013). "The Politics Of Bitcoin Mixing Services". *forbes.com* (Forbes). Retrieved 2 April 2014.
- [79] Bar-El, Hagai (3 April 2014). "Bitcoin does not provide anonymity". Archived from the original on 7 April 2014. Retrieved 26 April 2015.
- [80] 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.
- [81] Miers, Ian; Garman, Christina; Green, Matthew; Rubin, Aviel. "ZeroCoin: Anonymous Distributed E-Cash from Bitcoin" (PDF). Johns Hopkins University. Retrieved 15 February 2015.
- [82] Greenberg, Andy (29 April 2014). "'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever". *Wired*. Retrieved 15 February 2015.
- [83] Peterson, Andrea (3 January 2014). "Hal Finney received the first Bitcoin transaction. Here's how he describes it.". *The Washington Post*.
- [84] Popper, Nathaniel (30 August 2014). "Hal Finney, Cryptographer and Bitcoin Pioneer, Dies at 58". *NYTimes*. Retrieved 2 September 2014.
- [85] Wallace, Benjamin (23 November 2011). "The Rise and Fall of Bitcoin". *Wired*. Retrieved 4 November 2013.
- [86] Johannes Henning; Robin Schreiber (9 July 2013). "Bitcoin Cloud Security Mechanisms Seminar" (PDF). *www.dcl.hpi.uni-potsdam.de*. Hasso Plattner Institute. Retrieved 15 February 2015.
- [87] Nakamoto, Satoshi. "Re overflow bug serious". *Bitcointalk*. Retrieved 1 February 2015.
- [88] Lee, Timothy (11 March 2013). "Major glitch in Bitcoin network sparks sell-off; price temporarily falls 23%". *arstechnica.com*. Retrieved 15 February 2015.
- [89] Skelton, Andy (15 November 2012). "Pay Another Way: Bitcoin". WordPress. Retrieved 24 April 2014.
- [90] Franceschi-Bicchierai, Lorenzo (18 April 2013). "OKCupid Now Accepts Bitcoin". Mashable. Retrieved 24 April 2014.
- [91] Jane McEntegart (26 January 2014). "TigerDirect is Now Accepting Bitcoin As Payment". Tom's hardware. Retrieved 28 August 2014.
- [92] Vaishampayan, Saumya (9 January 2014). "Bitcoin now accepted on Overstock.com through VC-backed Coinbase". *marketwatch.com*. Wall Street Journal. Retrieved 10 February 2014.
- [93] Biggs, John (11 June 2014). "Expedia Now Accepts Bitcoin For Your Crypto-Vacations". Techcrunch. Retrieved 12 June 2014.
- [94] Flacy, Mike (19 July 2014). "Dell, Newegg Start Accepting Bitcoin as Payment". Digital Trends. Retrieved 5 August 2014.
- [95] Tom Warren (11 December 2014). "Microsoft now accepts Bitcoin to buy Xbox games and Windows apps". *The Verge* (Vox Media). Retrieved 11 December 2014.
- [96] Chavez-Dreyfuss, Gertrude; Connor, Michael (28 August 2014). "Bitcoin shows staying power as online merchants chase digital sparkle". Reuters. Retrieved 28 August 2014.
- [97] Rainey Reitman (20 January 2011). "Bitcoin - a Step Toward Censorship-Resistant Digital Currency". Electronic Frontier Foundation. Retrieved 21 November 2014.
- [98] Cohn, Cindy (20 June 2011). "EFF and Bitcoin". Electronic Frontier Foundation. Retrieved 16 April 2014.
- [99] Cindy Cohn, Peter Eckersley, Rainey Reitman, and Seth Schoen (17 May 2013). "EFF Will Accept Bitcoins to Support Digital Liberty". Electronic Frontier Foundation. Retrieved 27 April 2014.
- [100] 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.
- [101] Farrell, Greg (3 October 2013). "FBI Snags Silk Road Boss With Own Methods". *Bloomberg* (New York). Retrieved 27 October 2013.
- [102] Kapur, Saranya (15 October 2013). "China's Google Is Now Accepting Bitcoin". *businessinsider.com*. Business Insider, Inc. Retrieved 26 December 2013.

- [103] 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.
- [104] “BBC News - 'Legitimate' Bitcoin’s value soars after Senate hearing”. *Bbc.co.uk*. 19 November 2013. Retrieved 10 January 2014.
- [105] Lee, Cyrus (22 November 2013). “China no plans yet to legalize use of Bitcoins”. *ZDNet*. Retrieved 27 November 2013.
- [106] Kelion, Leo (18 December 2013). “Bitcoin sinks after China restricts yuan exchanges”. *bbc.com* (BBC). Retrieved 20 December 2013.
- [107] “China bans banks from bitcoin transactions”. *The Sydney Morning Herald* (Reuters). 6 December 2013. Retrieved 31 October 2014.
- [108] “Baidu Stops Accepting Bitcoins After China Ban”. *Bloomberg* (New York). 7 December 2013. Retrieved 11 December 2013.
- [109] “China bars use of virtual money for trading in real goods”. *English.mofcom.gov.cn*. 29 June 2009. Retrieved 10 January 2014.
- [110] McMillan, Robert (29 October 2013). “Take a tour of Robocoin, the world’s first Bitcoin ATM”. *Wired*. Retrieved 31 October 2014.
- [111] Raskin, Max (18 November 2013). “U.S. Agencies to Say Bitcoins Offer Legitimate Benefits”. *Bloomberg*. Retrieved 24 November 2013.
- [112] Todd Wasserman (18 November 2013). “Bitcoin Tops \$600, Up 60x Over the Last Year”. *Mashable.com*. Retrieved 10 January 2014.
- [113] Joel Fensch (2 January 2014). “Bitcoin Set to Boom in Latin America”. *Blog.panampost.com*. Retrieved 7 January 2014.
- [114] Lee, Dave (27 January 2014). “US makes Bitcoin exchange arrests after Silk Road closure”. *bbc.co.uk* (BBC). Retrieved 28 January 2014.
- [115] “MtGox gives bankruptcy details”. *bbc.com*. BBC. 4 March 2014. Retrieved 13 March 2014.
- [116] Biggs, John (10 February 2014). “What’s Going On With Bitcoin Exchange Mt. Gox?”. *TechCrunch*. Retrieved 26 February 2014.
- [117] “MtGox bitcoin exchange files for bankruptcy”. *bbc.com*. BBC. 28 February 2014. Retrieved 18 April 2014.
- [118] Vigna, Paul (25 Feb 2014). “Five Things About Mt. Gox’s Crisis”. *The Wall Street Journal* (Dow Jones and Company). Retrieved 18 April 2014.
- [119] Swan, Noelle (28 February 2014). “MtGox bankruptcy: Bitcoin insiders saw problems with the exchange for months”. *csmirror.com*. The Christian Science Monitor. Retrieved 18 April 2014.
- [120] 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.
- [121] Srivastava, Shivam (6 January 2015). “Bitcoin exchange Bitstamp suspends service after security breach”. *reuters.com* (Reuters). Retrieved 24 January 2015.
- [122] Novak, Marja (9 January 2015). “Bitcoin exchange Bitstamp says to resume trading on Friday”. *reuters.com* (Reuters). Retrieved 24 January 2015.
- [123] Russel, Jon (January 25, 2015). “Coinbase Is Opening The First Regulated Bitcoin Exchange In The U.S.”. *TechCrunch*. *TechCrunch*. Retrieved 21 February 2015.
- [124] Popper, Nathaniel (January 28, 2015). “Coinbase, a Bitcoin Exchange, Is Operating Without Licenses So Far”. *New York Times* (New York Times). Retrieved 21 February 2015.
- [125] 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.
- [126] Joyner, April (25 April 2014). “How bitcoin is moving money in Africa”. *usatoday.com* (USA Today). Retrieved 25 May 2014.
- [127] 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.

- [128] “The magic of mining”. *The Economist*. 8 January 2015. Retrieved 13 January 2015.
- [129] “Free Exchange. Money from nothing. Chronic deflation may keep Bitcoin from displacing its rivals.”. *The Economist*. 15 March 2014. Retrieved 25 March 2014.
- [130] Cuthbertson, Anthony (4 February 2015). “Bitcoin now accepted by 100,000 merchants worldwide”. *International Business Times* (IBTimes Co., Ltd.). Retrieved 20 November 2015.
- [131] Carter, Stephen L. (29 Nov 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.
- [132] Satran, Richard (15 May 2013). “How Did Bitcoin Become a Real Currency?”. *Forbes*. Retrieved 22 December 2014.
- [133] 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.
- [134] Woodhill, Louis (4 November 2013). “Bitcoins Are Digital Collectibles, Not Real Money”. *Forbes*. Retrieved 27 January 2014.
- [135] Bergstra, J. A., Weijland, P. (February 2014). “Bitcoin: a money-like informational commodity” (PDF). *arXiv.org*. Cornell University. p. 26.
- [136] Bheemaiah, Kariappa. “Block Chain 2.0: The Renaissance of Money”. *Wired*. Retrieved 4 January 2016.
- [137] 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.
- [138] Shin, Laura (21 October 2015). “Q&A: Chain.com CEO Adam Ludwin On How Money Will Become Digital”. *Forbes*. Retrieved 4 January 2016.
- [139] “BitGo Partners With Powerhouse Kraken Bitcoin Exchange”. *Business Wire*. 10 November 2015. Retrieved 4 January 2016.
- [140] “PR7231-15”. *Press releases* (CFTC). 17 September 2015. Retrieved 21 September 2015.
- [141] “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.
- [142] Steadman, Ian (26 April 2013). “Study: 45 percent of Bitcoin exchanges end up closing”. *Wired*. Retrieved 28 April 2013.
- [143] Nermin Hajdarbegovic (24 March 2014). “Kraken Bitcoin Exchange Passes ‘Proof of Reserves’ Cryptographic Audit”. *CoinDesk*. Retrieved 13 January 2015.
- [144] 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.
- [145] Lauren Orsini (23 October 2013). “Here’s What Happened When I Bought Bitcoin In Person”. *Business Insider*. Retrieved 4 February 2014.
- [146] Jervis, Rick (20 February 2014). “Bitcoin ATMs come to USA”. *USA Today*. Retrieved 31 October 2014.
- [147] Williams, Mark T. (21 October 2014). “Virtual Currencies – Bitcoin Risk” (PDF). *World Bank Conference Washington DC*. Boston University. Retrieved 11 November 2014.
- [148] 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.
- [149] Wilkes, Tommy (11 April 2013). “Backer defends virtual currency Bitcoin after big fall”. *Reuters*. Retrieved 7 January 2014.
- [150] Lee, Timothy B. (4 November 2013). “Bitcoin Doesn't Have a Deflation Problem”. *Forbes*. Retrieved 27 January 2014.
- [151] Lee, Timothy B. (12 April 2013). “Bitcoin’s Volatility Is A Disadvantage, But Not A Fatal One”. *Forbes*. Retrieved 15 November 2014.

- [152] Michael J. Casey (30 April 2014). "Bloomberg to List Bitcoin Prices, Offering Key Stamp of Approval". *WSJ*. Retrieved 23 March 2015.
- [153] Colombo, Jesse (19 December 2013). "Bitcoin May Be Following This Classic Bubble Stages Chart". *Forbes*. Retrieved 7 January 2014.
- [154] Moore, Heidi (3 April 2013). "Confused about Bitcoin? It's 'the Harlem Shake of currency'". *theguardian.com*. The Guardian. Retrieved 2 May 2014.
- [155] 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.
- [156] Liu, Alec (19 March 2013). "When Governments Take Your Money, Bitcoin Looks Really Good". *Motherboard*. Retrieved 7 January 2014.
- [157] Lee, Timothy B. (11 April 2013). "An Illustrated History Of Bitcoin Crashes". *Forbes*. Retrieved 7 January 2014.
- [158] Ben Rooney (29 November 2013). "Bitcoin worth almost as much as gold". *CNN*. Retrieved 31 October 2014.
- [159] "Bitcoin prices remain below \$600 amid bearish chart signals". *nasdaq.com*. August 2014. Retrieved 31 October 2014.
- [160] Ember, Sydney (13 January 2015). "As Bitcoin's Price Slides, Signs of a Squeeze". *New York Times*. Retrieved 16 January 2015.
- [161] Price, Rob (16 January 2015). "Deep Web Drug Dealers Are Freaking Out About The Bitcoin Crash". *Business Insider*. Retrieved 18 January 2015.
- [162] Kearns, Jeff (4 December 2013). "Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value". *bloomberg.com* (Bloomberg LP). Retrieved 23 December 2013.
- [163] Quiggin, John (16 April 2013). "The Bitcoin Bubble and a Bad Hypothesis". *The National Interest*. Retrieved 31 October 2014.
- [164] Shiller, Robert (1 March 2014). "In Search of a Stable Electronic Currency". *New York Times*. Retrieved 31 October 2014.
- [165] Dan Caplinger (4 April 2013). "Bitcoin's History of Crushing Speculators". *The Motley Fool*. Retrieved 7 January 2014.
- [166] Barford, Vanessa (13 December 2013). "Bitcoin: Price v hype". *bbc.com* (BBC). Retrieved 23 December 2013.
- [167] Boesler, Matthew (7 March 2013). "ANALYST: The Rise Of Bitcoin Teaches A Tremendous Lesson About Global Economics". *Business Insider*. Retrieved 31 October 2014.
- [168] Posner, Eric (11 April 2013). "Bitcoin is a Ponzi scheme—the Internet's favorite currency will collapse.". *Slate*. Retrieved 1 April 2014.
- [169] Clinch, Matt (10 March 2014). "Roubini launches stinging attack on bitcoin". *CNBC*. Retrieved 2 July 2014.
- [170] Ott Ummelas and Milda Seputyte (31 Jan 2014). "Bitcoin 'Ponzi' Concern Sparks Warning From Estonia Bank". *bloomberg.com* (Bloomberg). Retrieved 1 April 2014.
- [171] 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.
- [172] Kaushik Basu (July 2014). "Ponzis: The Science and Mystique of a Class of Financial Frauds" (PDF). World Bank Group. Retrieved 30 October 2014.
- [173] Lubin, Gus (9 March 2014). "ROUBINI: 'Bitcoin Is A Ponzi Game And A Conduit For Criminal Activities'". *Business Insider*. Retrieved 1 April 2014.
- [174] Jonathon M. Trugman (15 February 2014). "Welcome to 21st-century Ponzi scheme: Bitcoin". *The New York Post* (NYP Holdings, inc.). Retrieved 13 December 2014.
- [175] Jim Gibson (21 April 2014). "Is Bitcoin a Ponzi Scheme". *Huffington Post* (TheHuffingtonPost.com, Inc.). Retrieved 21 November 2014.
- [176] Jeremy Kirk (18 December 2013). "Bitcoin: The virtual currency built on math, hope and hype". *PC World* (International Data Group). Retrieved 21 November 2014.
- [177] Mather, John (1 December 2013). "Ponzi Logic: Debunking Gary North". *The Libertarian Standard* (Jeffrey Tucker). Retrieved 12 Feb 2014.

- [178] “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.
- [179] Kevin Dowd (5 November 2014). “Bitcoin is bust: Why investors should abandon the doomed cryptocurrency”. *Opinion (City A.M.)*. Retrieved 6 November 2014.
- [180] Eoghan Macguire (14 November 2014). “Bitcoin: One year on from peak price, what does the future hold?”. *Future Finance (CNN)*. Retrieved 15 November 2014.
- [181] Williams, Mark T. (17 December 2013). “FINANCE PROFESSOR: Bitcoin Will Crash To \$10 By Mid-2014”. *businessinsider.com*. Business Insider. Retrieved 26 February 2014.
- [182] Steve H. Hanke (18 September 2014). “Bitcoin Charts, Finally”. *Huffington Post (TheHuffingtonPost.com, Inc.)*. Retrieved 21 November 2014.
- [183] Robin Sidel (1 December 2014). “How Mt. Gox Debacle Won Over a Bitcoin Convert”. *Markets (The Wall Street Journal)*. Retrieved 4 December 2014.
- [184] 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.
- [185] Schroeder, Stan (1 December 2013). “Cameron Winklevoss: Bitcoin Might Hit \$40,000 Per Coin”. *Mashable (New York)*. Retrieved 31 October 2014.
- [186] Everett Rosenfeld (14 Jan 2015). “Bitcoin keeps falling, and worries keep rising”. *CNBC*. Retrieved 24 January 2015.
- [187] Worstall, Tim (20 June 2011). “So, That’s the End of Bitcoin Then”. *Forbes*. Retrieved 18 January 2015.
- [188] Covert, Adrian (9 August 2011). “The Bitcoin Is Dying. Whatever.”. *Gizmodo Australia (Allure Media)*. Retrieved 18 January 2015.
- [189] Calore, Michael (24 December 2012). “Wired, Tired, Expired for 2012: From Stellar to Suck”. *Wired (Condé Nast)*. Retrieved 18 January 2015.
- [190] Jourdan, Stanislas (21 May 2013). “Game over, bitcoin. Where is the next human-based digital currency?”. *Ouishare Magazine*. Retrieved 18 January 2015.
- [191] Roose, Kevin (20 June 2013). “Bitcoin Sees the Grim Reaper”. *New York Magazine (New York Media LLC)*. Retrieved 18 January 2015.
- [192] Hadas, Edward (8 January 2014). “An early obituary for bitcoin”. *Reuters*. Retrieved 18 January 2015.
- [193] “Bitcoin is Dead”. *Streetinsider.com*. 26 February 2014. Retrieved 18 January 2015.
- [194] Last, Jonathan V. (5 March 2014). “Bitcoin Is Dead”. *The Weekly Standard (The Weekly Standard LLC)*. Retrieved 18 January 2015.
- [195] 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.
- [196] Owen, Taylor (24 March 2014). “Bitcoin Is Dead — Long Live Bitcoin”. *Vice News*. Retrieved 18 January 2015.
- [197] Kaminska, Izabella (19 September 2014). “Cult Markets: When the bubble bursts”. *Financial Times*.
- [198] Krantz, Matt (16 January 2015). “Bitcoin is headed to the ‘ash heap’”. *USA Today*. Retrieved 18 January 2015.
- [199] Sparkes, Matthew (15 January 2015). “Bitcoin might be dead. It doesn’t matter.”. *The Telegraph (London)*. Retrieved 18 January 2015.
- [200] Baraniuk, Chris (18 January 2016). “Bitcoin: Is the crypto-currency doomed?”. *BBC*. Retrieved 19 January 2016.
- [201] Greenhill, Peter (31 March 2015). “Reports of Bitcoin’s Death Have Been Greatly Exaggerated”. *The Huffington Post*. Retrieved 5 April 2015.
- [202] Velde, François (December 2013). “Bitcoin: A primer” (PDF). *Chicago Fed letter*. Federal Reserve Bank of Chicago. p. 4. Retrieved December 2013.
- [203] Paul Krugman (28 December 2013). “Bitcoin Is Evil”. *krugman.blogs.nytimes.com*. Retrieved 28 December 2013.
- [204] 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.

- [205] 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.
- [206] Sparkes, Matthew (2 December 2013). "Software activist calls for 'truly anonymous' Bitcoins to 'protect democracy'". London: Telegraph. Retrieved 27 December 2013.
- [207] Shankland, Stephen (10 December 2013). "PayPal president David Marcus: Bitcoin is good, NFC is bad". *CNET*. Retrieved 10 December 2013.
- [208] "Bill Gates: Bitcoin Is Exciting Because It's Cheap". Bloomberg L.P. 2 October 2014. Retrieved 12 November 2014.
- [209] Kyle Torpey (21 May 2014). "Peter Schiff Embraces Bitcoin at Euro Pacific Precious Metals". *CryptoCoinsNews*. Retrieved 12 December 2014.
- [210] Pomela, Marina (10 April 2015). "Taxation on Bitcoin". The Brazil Business. Retrieved 18 September 2015.
- [211] Kahn, Jeremy (8 September 2015). "Isle of Man tax haven with tailless cats becomes bitcoin hub". Bloomberg. Retrieved 18 September 2015.
- [212] Masters, Daniel (10 July 2014). "Jersey Approves First Regulated Bitcoin Fund". *News* (BBC). Retrieved 9 September 2015.
- [213] Hancock, Edith (27 July 2015). "David Cameron to take UK fintech leaders on Asian tour". City A.M. Retrieved 18 September 2015.
- [214] Allison, Ian (1 July 2015). "Barclays talks Blockchain, BitCoin, and Distributed Ledgers". *Technology* (International Business Times). Retrieved 9 September 2015.
- [215] Ferenstein, Gregory (29 July 2015). "Former Obama Tech Advisor Explains How BitCoin Could Transform Government...". "*Ferenstein Wire*" (Forbes). Retrieved 9 September 2015.
- [216] 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.
- [217] "Clearly Canadian Joins Bitcoin Community". *finance.yahoo.com*. Yahoo! Finance. 23 December 2013. Retrieved 10 February 2014.
- [218] Sydney Ember (18 July 2014). "Dell Begins Accepting Bitcoin". *New York Times*. Retrieved 18 July 2014.
- [219] Casey, Michael (May 29, 2014). "Dish Network to Accept Bitcoin Payments". *The Wall Street Journal* (Dow Jones & Company). Retrieved 15 February 2015.
- [220] Mat 'Inferiorego' Elfring (17 September 2014). "Dynamite Digital Adds Bitcoin Payment Option and Offers Discount Bundle". CBS Interactive. Retrieved 27 December 2014.
- [221] Paul Vigna (11 June 2014). "Expedia Starts Accepting Bitcoin for Hotel Bookings". *Money Beat* (The Wall Street Journal). Retrieved 27 July 2014.
- [222] "Newegg accepts bitcoins". *newegg.com*. 1 July 2014. Retrieved 3 July 2014.
- [223] Sparkes, Matthew (10 January 2014). "Ten places where you can spend your bitcoins in the UK". *The Telegraph* (London). Retrieved 10 September 2013.
- [224] Davidson, Kavitha (16 Jan 2014). "How Many Bitcoins for a Courtside Seat?". *bloomberg.com* (Bloomberg LP). Retrieved 20 January 2014.
- [225] Ember, Sydney (16 December 2014). "Time Inc. begins accepting bitcoin payments". *Dealbook* (The New York Times). Retrieved 9 January 2015.
- [226] Holpuch, Amanda (22 November 2013). "Virgin Galactic to accept Bitcoin for space flights". *The Guardian*. Retrieved 24 November 2013.
- [227] Kharif, Olga (6 Jan 2014). "Bitcoin Tops \$1,000 Again as Zynga Accepts Virtual Money". *bloomberg.com* (Bloomberg LP). Retrieved 20 January 2014.
- [228] Stephanie Lo and J. Christina Wang (September 2014). "Bitcoin as Money?" (PDF). *Current Policy Perspectives (Federal Reserve Bank of Boston)* **14** (1): 6.
- [229] Scott Ellison (23 September 2014). "PayPal and Virtual Currency". PayPal. Retrieved 31 October 2014.

- [230] Cassidy Sharp (22 September 2014). "Greenpeace now accepting bitcoin donations". Greenpeace. Retrieved 31 October 2014.
- [231] 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.
- [232] Lisa Gruwell (30 July 2014). "Wikimedia Foundation Now Accepts Bitcoin". Wikimedia. Retrieved 30 October 2014.
- [233] 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.
- [234] Vigna, Paul (22 November 2013). "The University of Bitcoin Rises in Cyprus". *The Wall Street Journal*. Retrieved 22 November 2013.
- [235] Gertrude Chavez-Dreyfuss and Michael Connor (11 Dec 2014). "All the rage a year ago, bitcoin sputters as adoption stalls". *reuters.com* (Thompson Reuters). Retrieved 30 June 2015. bitcoin.
- [236] Robin Sidel (22 December 2013). "Banks Mostly Avoid Providing Bitcoin Services". Wallstreet Journal. Retrieved 27 December 2014.
- [237] Dougherty, Carter (5 December 2013). "Bankers Balking at Bitcoin in U.S. as Real-World Obstacles Mount". *bloomberg.com* (Bloomberg). Retrieved 16 April 2014.
- [238] "Bitcoin firms dumped by National Australia Bank as 'too risky'". *Australian Associated Press*. The Guardian. 10 April 2014. Retrieved 23 February 2015.
- [239] Weir, Mike (1 December 2014). "HSBC severs links with firm behind Bitcoin fund". *bbc.com*. BBC. Retrieved 9 January 2015.
- [240] Hill, Kashmir (5 December 2013). "Bitcoin Valued At \$1300 By Bank of America Analysts". *Forbes.com*. Retrieved 23 March 2014.
- [241] "Bitcoin: is Circle the world's first crypto-currency bank?". *The week.co.uk*. 16 May 2014. Retrieved 13 June 2014.
- [242] Salyer, Kirsten (20 March 2013). "Fleeing the Euro for Bitcoins". Bloomberg L.P. Retrieved 31 October 2014.
- [243] "Jersey approve Bitcoin fund launch on island". BBC news. 10 July 2014. Retrieved 10 July 2014.
- [244] Nathaniel Popper and Peter Lattman (11 April 2013). "Never Mind Facebook; Winklevoss Twins Rule in Digital Money". The New York Times. Retrieved 31 October 2014.
- [245] Grocer, Stephen (2 July 2013). "Beware the Risks of the Bitcoin: Winklevii Outline the Downside". *Moneybeat* (The Wall Street Journal). Retrieved 21 October 2013.
- [246] Popper, N. and Ember, S. (23 Jan 2015). "Winklevoss Twins aim to take Bitcoin Mainstream". *Dealbook blog* (The New York Times). Retrieved 15 February 2015.
- [247] Tepper, Fitz (5 October 2015). "Winklevoss Twins Receive Approval To Launch Bitcoin Exchange Gemini". TechCrunch. Retrieved 22 November 2015.
- [248] Curran, Rob (6 July 2015). "A Bitcoin Fund Is Born, With Teething Pains". *Markets* (The Wall Street Journal). Retrieved 22 November 2015.
- [249] Shin, Laura (11 December 2015). "Should You Invest In Bitcoin? 10 Arguments In Favor As Of December 2015". Forbes. Retrieved 12 December 2015.
- [250] Jonathan Stempel (11 March 2014). "Beware Bitcoin: U.S. brokerage regulator.". *reuters.com*. Retrieved 14 March 2014.
- [251] Hill, Kashmir. "How You Should Have Spent \$100 In 2013 (Hint: Bitcoin)". *Forbes*. Retrieved 16 Feb 2015.
- [252] Steverman, Ben (Dec 23, 2014). "The Best and Worst Investments of 2014". *bloomberg.com* (Bloomberg LP). Retrieved 9 January 2015.
- [253] Gilbert, Mark (29 December 2015). "Bitcoin Won 2015. Apple ... Did Not". Bloomberg. Retrieved 29 December 2015.
- [254] CNBC (30 April 2014). "Bloomberg terminal now following bitcoin prices". Retrieved 23 March 2015.
- [255] "NYSE to Launch NYSE Bitcoin Index, NYXBT". *businesswire.com*. Business Wire. May 19, 2015. Retrieved 22 May 2015.
- [256] Simonite, Tom (12 June 2013). "Bitcoin Millionaires Become Investing Angels". *Computing News* (MIT Technology Review). Retrieved 13 June 2013.

- [257] Robin Sidel (1 December 2014). "Ten-hut! Bitcoin Recruits Snap To". *Wall Street Journal* (Dow Jones & Company). Retrieved 9 December 2014.
- [258] Alex Hern (1 July 2014). "Silk Road's legacy 30,000 bitcoin sold at auction to mystery buyers". *The Guardian*. Retrieved 31 October 2014.
- [259] "CoinSeed raises \$7.5m, invests \$5m in Bitcoin mining hardware – Investment Round Up". *Red Herring*. 24 January 2014. Retrieved 9 March 2014.
- [260] Matonis, Jon (3 November 2012). "ECB: "Roots Of Bitcoin Can Be Found In The Austrian School Of Economics"". *Forbes*. Retrieved 18 September 2015.
- [261] Friedrich von Hayek (October 1976). *Denationalisation of Money: The Argument Refined* (PDF). 2 Lord North Street, Westminster, London SW1P 3LB: The institute of economic affairs. ISBN 0-255 36239-0. Retrieved 10 September 2015.
- [262] Doug Henwood (19 May 2014). "Bitcoin the Future of Money?". *The Nation.com*. Retrieved 12 September 2014.
- [263] Matthew Graham Wilson and Aaron Yelowitz (November 2014). "Characteristics of Bitcoin Users: An Analysis of Google Search Data". *Social Science Research Network*. Working Papers Series.
- [264] Brett Scott (1 June 2014). "Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain". *E-International Relations*. Retrieved 31 October 2014.
- [265] Margaret Corvid (December 2013). "A left defence of Bitcoin". *International Socialist Network*. Retrieved 31 October 2014.
- [266] Melanie L. Fein (15 February 2013). "The Shadow Banking Charade". Retrieved 31 October 2014.
- [267] Edward Hadas (27 November 2013). "Right-wing dreams". *Thomson Reuters*. Retrieved 31 October 2014.
- [268] Hamill, Jasper (19 December 2013). "Native American Activist Wants To Swap The Dollar For Bitcoin". *Forbes*. Retrieved 1 October 2014.
- [269] Staff (10 January 2015). "Much more than digital cash". *The Economist* (The Economist Newspaper Ltd). Retrieved 13 January 2015.
- [270] Strauss, Steven (14 April 2013). "Nine Trust-Based Problems With Bitcoin". *The Huffington Post*. Retrieved 20 October 2013.
- [271] AFP (15 Sep 2014). "Why Bangladesh will jail Bitcoin traders". *telegraph.co.uk* (London: The Telegraph). Retrieved 23 February 2015.
- [272] 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.
- [273] Cuthbertson, Anthony (1 September 2014). "Ecuador Reveals National Digital Currency Plans Following Bitcoin Ban". *ibtimes.co.uk*. *International Business Times*. Retrieved 23 February 2015.
- [274] 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.
- [275] Sanati, Cyrus (18 December 2012). "Bitcoin looks primed for money laundering". *money.cnn.com* (CNN). Retrieved 18 October 2013.
- [276] "Monetarists Anonymous". *The Economist* (The Economist Newspaper Limited). 29 September 2012. Retrieved 21 October 2013.
- [277] 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.
- [278] Jeffries, Adrienne (19 December 2013). "How to steal Bitcoin in three easy steps". *The Verge*. Retrieved 17 January 2014.
- [279] Everett, David (April 2012). "So how can you steal Bitcoins". *Smartcard & Identity News*. Retrieved 17 January 2014.
- [280] Hern, Alex (9 December 2013). "Recovering stolen bitcoin: a digital wild goose chase". *The Guardian*. Retrieved 6 March 2014.
- [281] "Silk Road 2 loses \$2.7m in bitcoins in alleged hack". *BBC News*. 14 February 2014. Retrieved 15 February 2014.

- [282] Hern, Alex (8 November 2013). "Bitcoin site Inputs.io loses £1m after hackers strike twice". *The Guardian*. Retrieved 18 September 2015.
- [283] 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.
- [284] Truong, Alice (6 March 2014). "Another Bitcoin exchange, another heist". *Fast Company*. Retrieved 7 March 2014.
- [285] Zack Whittaker (5 January 2015). "Bitstamp exchange hacked, \$5M worth of bitcoin stolen". *Zdnet*. CBS Interactive. Retrieved 6 January 2015.
- [286] Millward, Steven (Feb 16, 2015). "Nearly \$2M in bitcoins feared lost after Chinese cryptocurrency exchange hack". *techinasia.com*. Tech In Asia. Retrieved 18 February 2015.
- [287] 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
- [288] Schweizer, Kristen (10 October 2014). "Bitcoin Payments by Pedophiles Frustrate Child Porn Fight". *BloombergBusiness* (Bloomberg LP). Retrieved 16 February 2015.
- [289] 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.
- [290] Smith, Gerry (15 April 2013). "How Bitcoin Sales Of Guns Could Undermine New Rules". *huffingtonpost.com* (TheHuffingtonPost.com, Inc.). Retrieved 20 October 2013.
- [291] *Faking Murders And Stealing Bitcoin: Why The Silk Road Is The Strangest Crime Story Of The Decade*, retrieved 2 Januari 2016 Check date values in: |access-date= (help)
- [292] 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.
- [293] Kelion, Leo (12 February 2014). "Five arrested in Utopia dark net marketplace crackdown". *bbc.co.uk* (BBC). Retrieved 13 February 2014.
- [294] 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
- [295] Robert McMillan (2 October 2013). "Bitcoin Values Plummet \$500M, Then Recover, After Silk Road Bust". *Wired*. Retrieved 31 October 2014.
- [296] "Silk Road drug website founder Ross Ulbricht jailed". *BBC News*. BBC. 29 May 2015. Retrieved 30 May 2015.
- [297] Katie Silver (31 March 2014). "Silk Road closure fails to dampen illegal drug sales online, experts say". *ABC News*. Retrieved 31 October 2014.
- [298] 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.
- [299] Wakefield, Jane (7 November 2014). "Huge raid to shut down 400-plus dark net sites". *bbc.com*. BBC. Retrieved 8 November 2014.
- [300] Nate Raymond (19 December 2014). "Bitcoin backer gets two years prison for illicit transfers". *Reuters* (Thompson Reuters). Retrieved 20 December 2014.
- [301] "Ross Ulbricht: Silk Road creator convicted on drugs charges". *BBC*. 5 February 2015. Retrieved 17 February 2015.
- [302] 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.
- [303] "While Markets Get Seized: Pedophiles Launch a Crowdfunding Site". Retrieved 19 Feb 2015.
- [304] Hopkins, Curt (7 May 2013). "If you own Bitcoin, you also own links to child porn". *The Daily Dot*. Retrieved 16 February 2015.

- [305] Bradbury, Danny. "As Bitcoin slides, the Blockchain grows". IET Engineering and Technology Magazine.
- [306] 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.
- [307] "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.
- [308] "SEC charges Texas man with running Bitcoin-denominated Ponzi scheme" (Press release). US Securities and Exchange Commission. 23 July 2013. Retrieved 7 March 2014.
- [309] Jay Adkisson (25 September 2014). "Bitcoin Savings & Trust Comes Up \$40 Million Short On The Trust Part". *Personal Finance* (Forbes). Retrieved 13 December 2014.
- [310] Greenburg, Andy (26 April 2014). "Nearly 150 Breeds Of Bitcoin-Stealing Malware In The Wild, Researchers Say". *forbes.com* (Forbes). Retrieved 9 January 2015.
- [311] Peter Coogan (17 June 2011). "Bitcoin Botnet Mining". *Symantec.com*. Retrieved 24 January 2012.
- [312] Goodin, Dan (16 August 2011). "Malware mints virtual currency using victim's GPU". *The Register*. Retrieved 31 October 2014.
- [313] Ryder, Greg (9 June 2013). "All About Bitcoin Mining: Road To Riches Or Fool's Gold?". Tom's hardware. Retrieved 18 September 2015.
- [314] "Infosecurity - Researcher discovers distributed bitcoin cracking trojan malware". *Infosecurity-magazine.com*. 19 August 2011. Retrieved 24 January 2012.
- [315] 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.
- [316] "E-Sports Entertainment settles Bitcoin botnet allegations". *BBC News*. 20 November 2013. Retrieved 24 November 2013.
- [317] 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.
- [318] McGlaun, Shane (9 January 2014). "Yahoo malware turned Euro PCs into bitcoin miners". *SlashGear*. Retrieved 8 January 2015.
- [319] Liat Clark (20 January 2014). "Microsoft stopped Tor running automatically on botnet-infected systems". Retrieved 8 January 2015.
- [320] Hornyack, Tim (6 June 2014). "US researcher banned for mining Bitcoin using university supercomputers". *PC world.com* (IDG Consumer & SMB). Retrieved 13 June 2014.
- [321] Hajdarbegovic, Nermin (27 February 2014). "Nearly 150 strains of malware are after your bitcoins". *CoinDesk*. Retrieved 7 March 2014.
- [322] Gregg Keizer (28 February 2014). "Bitcoin malware count soars as cryptocurrency value climbs". *Computerworld*. Retrieved 8 January 2015.
- [323] Zach Miners (24 Feb 2014). "Bitcoins, other digital currencies stolen in massive 'Pony' botnet attack". Retrieved 8 January 2015.
- [324] Finkle, Jim (24 February 2014). "'Pony' botnet steals bitcoins, digital currencies: Trustwave". *Reuters*. Retrieved 7 March 2014.
- [325] "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.
- [326] "How Ransomware turns your computer into a bitcoin miner". *The Guardian*. 10 February 2014. Retrieved 7 March 2014.
- [327] Gibbs, Samuel (21 November 2013). "US police force pay bitcoin ransom in Cryptolocker malware scam". *The Guardian*. Retrieved 7 March 2014.
- [328] Erik Bonadonna (29 March 2013). "Bitcoin and the Double-spending Problem". Cornell University. Retrieved 22 October 2014.

- [329] 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.
- [330] Michael J. Casey; Paul Vigna (16 June 2014). "Short-Term Fixes To Avert "51% Attack"". *Money Beat* (Wall Street Journal). Retrieved 30 June 2014.
- [331] Eyal, Ittay; Sirer, Emin Gun (15 November 2013). "Majority is not Enough: Bitcoin Mining is Vulnerable". Retrieved 7 October 2014.
- [332] Hill, Kashmir (6 November 2013). "Bitcoin Is Not Broken". *Forbes*. Retrieved 19 October 2014.
- [333] Eyal, Ittay; Sirer, Emin Gun (8 November 2013). "Response to Fairweather Mining". Retrieved 28 May 2015.
- [334] Eyal, Ittay; Sirer, Emin Gun (14 November 2013). "Response to Fairweather Mining". Retrieved 28 May 2015.
- [335] Reid, Fergal; Harrigan, Martin (2013). "An Analysis of Anonymity in the Bitcoin System". *Security and Privacy in Social Networks*: 197–223.
- [336] Biryukov, Alex; Khovratovich, Dmitry; Pustogarov, Ivan (2014). "Deanonymisation of clients in Bitcoin P2P network". *ACM Conference on Computer and Communications Security*.
- [337] Higginbotham, Stacey (9 September 2014). "Check out IBM's proposal for an internet of things architecture using Bitcoin's block chain tech". *gigaom.com*. Gigaom. Retrieved 29 April 2015.
- [338] Barker, Colin (21 January 2015). "Is blockchain the key to the Internet of Things? IBM and Samsung think it might just be". ZDNet. Retrieved 29 April 2015.
- [339] Gertrude Chavez-Dreyfuss (Mar 12, 2015). "IBM looking at adopting bitcoin technology for major currencies". *Reuters*. Retrieved 13 March 2015.
- [340] Hern, Alex (13 May 2015). "Nasdaq bets on bitcoin's blockchain as the future of finance". *theguardian.com*. The Guardian. Retrieved 22 May 2015.
- [341] Shin, Laura (24 June 2015). "Nasdaq Selects Bitcoin Startup Chain To Run Pilot In Private Market Arm". *Forbes*. Retrieved 25 June 2015.
- [342] Chavez-Dreyfuss, Gertrude (15 May 2015). "Honduras to build land title registry using bitcoin technology". *Yahoo News*. Retrieved 22 June 2015.
- [343] "How porn links and Ben Bernanke snuck into Bitcoin's code". *CNN Money* (CNN). 2 May 2013.
- [344] Hern, Alex (30 April 2014). "MIT students to get \$100 worth of bitcoin from Wall Street donor". *The Guardian*. Retrieved 1 May 2014.
- [345] Dan (29 April 2014). "Announcing the MIT Bitcoin Project". MIT Bitcoin Club. Retrieved 4 July 2015.
- [346] "MAK Vienna Becomes First Museum to Use Bitcoin to Acquire Art, a Harm van den Dorpel | ARTnews". *www.artnews.com*. Retrieved 2015-12-29.
- [347] Kenigsberg, Ben (2 October 2014). "Financial Wild West". *nytimes.com* (New York Times). Retrieved 8 May 2015.
- [348] 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.
- [349] ...[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)
- [350] "Bitcoin Parte 1". Radio Educación. 25 April 2013. Retrieved 19 September 2015.
- [351] "Bitcoin Parte 2". Radio Educación. 25 April 2013. Retrieved 19 September 2015.
- [352] Jason Kurtz (February 20, 2015). "Buying bitcoin: Morgan Spurlock looks to live off online currency". CNN. Retrieved 25 February 2015.
- [353] "The Good Wife: Season 3, Episode 13 Bitcoin for Dummies (15 Jan. 2012)". *imdb.com*. IMDb. Retrieved 8 May 2015.
- [354] dinbits (October 18, 2015). "Judge Judy's Bitcoin Case". dinbits. Retrieved 18 October 2015.

1.1.15 External links

- Bitcoin at DMOZ
- Bitcoin video series at Khan Academy
- Bitcoin: a cryptographic currency Bitcoin, Instituto Nacional de Tecnologías de la Comunicación (INTECO), Spain, or National Institute of Communication Technologies (undated, 47pp, in English).
- Quandl - Bitcoin currency data - historical statistics in time series downloadable format.

1.2 Mastercoin

Omni (formerly **Mastercoin**) is a digital currency and communications protocol built on the bitcoin block chain. It is one of several efforts to enable complex financial functions in a cryptocurrency.^[1] Planned features include the development of a decentralized exchange and the implementation of smart property and savings wallets.^[2]

J. R. Willett published the first draft of the Mastercoin protocol in January 2012 as a white paper, in which he proposed that existing bitcoin protocol “can be used as a protocol layer, on top of which new currency layers with new rules can be built without changing the foundation.”^[2]

The Mastercoin project officially launched on July 31, 2013, with a month-long fundraiser in which anyone could buy Mastercoins - the digital tokens that the protocol uses to conduct transactions – by sending bitcoins to a special “Exodus Address”.^[2] The idea was that as the platform was being developed, the tokens would become more valuable and investors could sell their Mastercoins to realize a return.^[3] A nonprofit organization called the Mastercoin Foundation was formed to handle the funds sent to the address.^[2] Despite warnings that Mastercoin might just be an elaborate scam, some 500 people invested,^[4] sending a total of about 5000 bitcoins worth about US\$500,000 at the time.^[5]

As of January 2014, J.R. Willet is employed full-time by the Mastercoin Foundation as “chief architect”^[6]

As of February 2014, Mastercoin was the world’s seventh largest cryptocurrency by market capitalization according to coinmarketcap.com.^[7]

In April 2014, MaidSafe used a crowdsale to raise over \$7,000,000 in Mastercoins and bitcoins. The value of the Mastercoins (half the currency) subsequently declined, leaving the total from the sale at \$5,500,000.^{[8][9]} In July, MaidSafe COO Nick Lambert was among a number of people joining the Mastercoin board as observers.^[10]

In March 2015 Mastercoin efforts were rebranded as Omni.^[11] Omni role in bitcoin ecosystem is declared as being a platform for decentralized protocols like Factom and MaidSafe.^[12] «A common analogy that is used to describe the relation of the Omni Layer to bitcoin is that of HTTP to TCP/IP: HTTP, like the Omni Layer, is the application layer to the more fundamental transport and internet layer of TCP/IP, like bitcoin.»^[13]

1.2.1 References

- [1] “Bitcoin is not just digital currency. It’s Napster for finance. - Term Sheet”. Finance.fortune.cnn.com. 2014-01-21. Retrieved 2014-02-24.
- [2] Buterin, Vitalik (4 November 2013). “Mastercoin: A Second-Generation Protocol on the Bitcoin Blockchain”. *Bitcoin Magazine*. Retrieved 9 January 2014.
- [3] Chernova, Yuliya. “New Use for Bitcoin: Compensation for Open-Source Software Development”. The Wall Street Journal. Retrieved 13 February 2014.
- [4] Hamill, Jasper (30 November 2013). “Fed Up With Bitcoin? Here’s How To Start Your Own Currency”. *Forbes*. Retrieved 13 February 2014.
- [5] Nermin Hajdarbegovic (2013-12-06). “Mastercoin Foundation Lets Virtual Currencies use Bitcoin Protocol”. Coin-desk.com. Retrieved 2014-02-24.
- [6] “Master Protocol Creator J.R. Willett Joins Mastercoin Foundation as Full-Time Chief Architect”. Mastercoin Foundation. Retrieved 2014-02-24.
- [7] Paul Vigna (2014-02-14). “BitBeat: Bitcoin Exchanges Finally Getting Some Relief”. WSJ.com. Retrieved 2014-02-27.

- [8] Bradbury, Danny (25 June 2014). "MaidSafe COO Reflects on Lessons Learned from Crowdsale". *CoinDesk*. Retrieved 28 July 2014.
- [9] Hill, Kashmir (3 June 2014). "The First 'Bitcoin 2.0' Crowd Sale Was A Wildly Successful \$7 Million Disaster". *Forbes*. Retrieved 28 July 2014.
- [10] Wilmoth, Josiah (15 July 2014). "Weekly Altcoin News Update: Brock Pierce Resigns from Mastercoin Foundation and a Nxt Stakeholder Posts a 500 Bitcoin Bounty". *CryptoCoins News*. Retrieved 28 July 2014.
- [11] "The Omni Layer official site".
- [12] Rizzo, Pete (2015-01-21). "Mastercoin Seeks Second Start With Omni Reboot". *CoinDesk*. Retrieved 2015-03-23.
- [13] "Omni Layer GitHub". *GitHub.com*. Retrieved 2015-03-23.

1.2.2 External links

- Official website

1.3 MazaCoin

Mazacoin was developed by the BTC Oyate Initiative, under the direction of Payu Harris, a native American activist, web developer, and digital currency trader who has traced his ancestry to the Northern Cheyenne tribe.^[1] Harris hopes that the currency will cause the international community to "realize we're serious about our sovereignty", as well as help alleviate poverty within the nation.^{[2][3]}

The digital currency is a type of cryptocurrency, and like the cryptocurrency bitcoin, MazaCoin can be bought or sold on international cryptocurrency exchanges, or it can be obtained through virtual "mining".^{[1][4]} The underlying software for MazaCoin is derived from that of another cryptocurrency, ZetaCoin, which in turn is based on bitcoin's SHA-256 proof of work system.^{[5][6]} It includes 50 million pre-mined Mazacoin, equally split by the Lakota Nation between a national reserve and a planned "Tribal Trust",^[5] which it is hoped will help "to prevent the wild speculation that has caused bitcoin such price volatility."^[7] One of its differences from bitcoin is that it is inflationary; while there is a maximum cap of 21 million bitcoins that will be produced, there is no similar cap for MazaCoin.^[8] The Lakota Nation anticipates that 2.4 billion MazaCoin will be produced within five years, and drop to 1 million MazaCoin per year thereafter.^[8] Another difference from bitcoin is that it is "simpler" in a way that makes it consume less power to run the cryptographic mining algorithm, making it more environmentally friendly.^[8]

The MazaCoin development received a Memorandum of Understanding between the Oglala Lakota Nation & the MazaCoin Development Team.^[9] On 25 March 2014, David Mills, Director Oglala Sioux Tribe, Office of Economic Development commented on the status of MazaCoin that the tribe is "for support of more research" and "if we are satisfied with the outcome we will develop a resolution to the Tribal E&BD Committee in support of this venture to be forwarded on the Tribal Council for final approval."^[10]

The MazaCoin development team officially endorsed a community-built and -driven website called MazaTalk.^[11]

"This coin has a block target of 120 seconds, and a block reward of 1000 MZC, halving now every 950,000 blocks. The initial block reward was 5000MZC, which was lowered to 1000MZC at block 100,000 when the difficulty re-targeting algorithm was changed in Mazacoin"^[6]

1.3.1 References

- [1] Hamill, Jasper (2014-02-27). "The Battle of Little Bitcoin: Native American tribe launches its own cryptocurrency". *Forbes*.
- [2] Gaylord, Chris (2014-03-22). "Good Reads: From teacher fundraisers, to an atomic timekeeper, to MazaCoin". *The Christian Science Monitor*.
- [3] Landry, Alysa (2014-03-03). "9 questions surrounding MazaCoin, the Lakota cryptocurrency: answered". *Indian Country Today Media Network*.
- [4] Ramos, Jairo (2014-03-07). "A Native American tribe hopes digital currency boosts its sovereignty". *Code Switch: Frontiers of Race, Culture, and Ethnicity* (National Public Radio).

- [5] Hofman, Adam (2014-03-06). "The dawn of the national currency – an exploration of country-based cryptocurrencies". *Bitcoin Magazine*.
- [6] Bradbury, Danny (2014-02-06). "Mazacoin Aims to be Sovereign Altcoin for Native Americans". *CoinDesk*.
- [7] Jeffries, Adrienne (2014-03-05). "Native American tribes adopt Bitcoin-like currency, prepare to battle US government". *The Verge*.
- [8] Vincent, James (2014-03-03). "Mazacoin: Native American tribe adopts bitcoin derivative as 'national currency'". *The Independent*.
- [9] "Memorandum of Understanding between the Oglala Lakota Nation & the MazaCoin Development Team". Retrieved 2014-03-25. Document published by unknown user on Google Docs website.
- [10] "David Mills, Director Oglala Sioux Tribe, Office of Economic Development on the status of MazaCoin". Mazatalk.com. Retrieved 2014-03-25.
- [11] "Statement By The MazaCoin Development Team On The New Website MazaTalk". Retrieved 2014-03-25. Statement posted by anonymous user "Guest" on Pastebin website.

1.3.2 External links

- Official website
- Officially endorsed community website MazaTalk.com
- "Crypto-Currency: Lakota Nation set to launch MazaCoin", O'Gorman, Helen. Financial Crime Asia (website). 19 February 2014.

1.4 Namecoin

Namecoin (Symbol: **N** or **NMC**) is a cryptocurrency and the first fork of the bitcoin software.^{[1][3][2][4]} It is based on the code of bitcoin and uses the same proof-of-work algorithm. It is limited to 21 million coins.^[6]

Unlike bitcoin, Namecoin can store data within its own blockchain transaction database. The original proposal for Namecoin called for Namecoin to insert data into bitcoin's block chain directly.^[7] Anticipating scaling difficulties with this approach,^[8] a shared proof-of-work (POW) system was proposed to secure new cryptocurrencies with different use cases.^[9]

Namecoin's flagship use case is the censorship-resistant top level domain `.bit`, which is functionally similar to `.com` or `.net` domains but is independent of ICANN, the main governing body for domain names.^[10]

1.4.1 Records

Each Namecoin record consists of a key and a value which can be up to 520 bytes in size. Each key is actually a path, with the namespace preceding the name of the record. The key `d/example` signifies a record stored in the DNS namespace `d` with the name `example` and corresponds to the record for the `example.bit` website. The content of `d/example` is expected to conform to the DNS namespace specification.^[11]

The current fee for a record is 0.01 NMC and records expire after 36000 blocks (~200 days) unless updated or renewed. Namecoins used to purchase records are marked as used and destroyed, as giving the fee to miners would enable larger miners to register names at a significant discount.^[12]

1.4.2 Uses

Proposed potential uses for Namecoin besides domain name registration include:

- Identity systems^[13]
- Messaging systems^{[14][15]}

- Personal namespaces^[16]
- Notary/timestamp systems^[17]
- Alias systems^{[18][19]}
- Issuance of shares/stocks^{[20][21]}

1.4.3 History

In September 2010 a discussion was started in the Bitcointalk forum about a hypothetical system called BitDNS and generalizing bitcoin, based on a talk at IRC at 14 November 2010. Gavin Andresen and Satoshi Nakamoto joined the discussion in the Bitcointalk forum and supported the idea of BitDNS.^{[22][23][24]} A reward for implementing BitDNS was announced at the Bitcointalk forum in December 2010.^[25] Soon a developer decided to implement this idea to earn this reward.^{[25][26]} On April 18, 2011 Namecoin was introduced by Vined (Rumored to be Vincent Durham) as a multipurpose and distributed naming system based on bitcoin. It was inspired by the BitDNS discussion on the Bitcointalk forum.^[27] WikiLeaks mentioned the project via Twitter in June 2011.^[28]

Two years later, in June 2013, NameID was launched.^{[29][30]} It is a service to associate profile information with identities on the Namecoin blockchain and an OpenID provider to allow logging into existing websites with Namecoin identities. The main site itself is accompanied by an open protocol for password-less authentication with Namecoin identities, a corresponding free-software implementation and a supporting extension for Firefox.

In October 2013, Michael Gronager, main developer of libcoin,^[31] found a security issue in the Namecoin protocol, which allowed modifying foreign names. It was successfully fixed in a short timeframe and was never exploited, except for bitcoin.bit as a proof-of-concept.^{[32][33]}

In February 2014, a plug-in for Firefox compatible with Windows and Linux, FreeSpeechMe, was released, providing automatic resolution of .bit addresses. This is available by downloading the Namecoin block chain and running it in the background.^[34]

Namecoin was also mentioned by ICANN in a public draft report as the most well-known example of distributing control and privacy in DNS.^{[35][36]}

One month later, in March 2014, OneName was released. It is another identity system built on top of the Namecoin protocol that stores usernames and personal profile data in the Namecoin block chain.^[37] In contrast to NameID, OneName is built purely for profile information and does not support password-less authentication or log-in. OneName later (in September 2015) switched user profiles from Namecoin to the Bitcoin blockchain, citing the higher hashrate of Bitcoin as the reason.^[38]

In May 2014, Kevin McCoy and Anil Dash introduced Monegraph, a system that links Twitter accounts and digital assets (such as artwork) in the block chain, allowing proof of ownership of such assets.^[39]

1.4.4 See also

- Alternative DNS
- Zooko's Triangle

1.4.5 References

- [1] Isgur, Ben (2014-07-16). "A Little Altcoin Sanity: Namecoin". *CoinReport*.
- [2] "Namecoin – Next Generation Domain Name System". *CoinJoint*. 2014-06-05.
- [3] Buterin, Vitalik (2013-10-26). "Bitcoin in Israel, Part 3: Interview on Alternative Currencies". *Bitcoin Magazine*.
- [4] Brokaw, Alex (2014-08-23). "Crypto 2.0 Roundup: Bitcoin's Revolution Moves Beyond Currency". *CoinDesk*.
- [5] Gilson, David (2013-06-18). "What are Namecoins and .bit domains?". *CoinDesk*.
- [6] Loibl, Andreas (2014-08-01). "Namecoin" (PDF).
- [7] appamatto (2010-10-15). "BitDNS and Generalizing Bitcoin". *BitcoinTalk*.

- [8] Nakamoto, Satoshi (2010-12-10). "Re: BitDNS and Generalizing Bitcoin". *Bitcoin Talk*.
- [9] Nakamoto, Satoshi (2010-12-09). "Re: BitDNS and Generalizing Bitcoin". *BitcoinTalk*.
- [10] Dourado, Eli (2014-02-05). "Can Namecoin Obsolete ICANN (and More)?"'. *Theumlaut*.
- [11] "Namecoin DNS specification".
- [12] "Namecoin FAQ".
- [13] "Namespace:Identity". *Dot-Bit*.
- [14] "Messaging System]". *Dot-Bit*.
- [15] Namecoin block explorer, Archived here
- [16] "Personal Namespace". *Dot-Bit*.
- [17] Kirk, Jeremy (2013-05-24). "Could the Bitcoin network be used as an ultrasecure notary service?". *Techworld*.
- [18] ecdsa.org/bitcoin-alias/, Archived page
- [19] ecdsa.org/bitcoin_URIs.html, Archived page
- [20] Phelix. "Coming up: Namecoin Stock Control". *Namecoin forum*. Retrieved 2012-10-05.
- [21] Phelix (2014-01-12). "ANTPY - Atomic Name Trading". *Namecoin Forum*.
- [22] appamatto (2010-10-15). "BitDNS and Generalizing Bitcoin". *Bitcoin Forum*. Bitcointalk.org.
- [23] IRC (2010-10-14). "IRC discussion about BitDNS 1/2". web.archive.org. web.archive.org.
- [24] IRC (2010-10-15). "IRC discussion about BitDNS 2/2". web.archive.org. web.archive.org.
- [25] kiba (2010-04-12). "BitDNS Bounty (3500 BTC)". *Bitcoin Forum*. Bitcointalk.org.
- [26] "vinned/namecoin". *GitHub*. Retrieved 24 February 2015.
- [27] vinned (2011-04-18). "[announce] Namecoin - a distributed naming system based on Bitcoin". *Bitcoin Forum*. Bitcointalk.org.
- [28] "Twitter / wikileaks: Namecoin and Bitcoin will be ...". *WikiLeaks*, via *Twitter*. 2011-06-09. Retrieved 2014-05-20.
- [29] Kraft, Daniel (2013-07-25). "NameID - Use namecoin id/ to log into OpenID sites". *Namecoin Forum*.
- [30] Kraft, Daniel (2013-07-20). "Login mit Namecoin". *Bitcoin Forum*.
- [31] "libcoin/libcoin". *GitHub*. Retrieved 24 February 2015.
- [32] Gilson, David (2013-10-28). "Developers attempt to resurrect Namecoin after fundamental flaw discovered". *CoinDesk*.
- [33] libcoin (2011-04-18). "Namecoin was stillborn, I had to switch off life-support". *Bitcoin Forum*. Bitcointalk.org.
- [34] Reyes, Ferdinand (2014-02-13). "FreeSpeechMe: The new anti-censorship and secure domain resolving Namecoin-based plug-in". *Bitcoin Magazine*.
- [35] "The Internet Corporation for Assigned Names and Numbers Identifier Technology Innovation - Draft Report" (PDF). *ICANN*. 2014-02-21.
- [36] Hofman, Adam (2014-03-19). "Bitcoin and Namecoin Appear in Draft ICANN Report – U.S. Plans to Relinquish Remaining Control of Internet". *Bitcoin Magazine*.
- [37] Rizzo, Pete (2014-03-27). "How OneName Makes Bitcoin Payments as Simple as Facebook Sharing". *CoinDesk*.
- [38] onename (2015-09-15). "Why Onename is Migrating to the Bitcoin Blockchain". *OneName Blog*.
- [39] Cawrey, Daniel (2014-05-15). "How Monegraph Uses the Block Chain to Verify Digital Assets". *CoinDesk*.

1.4.6 External links

- Namecoin.info

1.5 NuBits

NuBits are the worlds first distributed, stable value digital currency.^[1] One NuBit is equal to one US dollar in value. It works like many other popular digital currencies without the risk of volatility.

NuBits are notable for being the first decentralized cryptocurrency to maintain a \$1.00 US price peg for a period of one year,^[2] having accomplished it on September 23, 2015.^[3] The Nu project is considered a global pioneer in the creation of decentralized stable-value cryptocurrencies.^[1]

Price is maintained by users placing huge market orders in both sides of 1 USD (or their equivalent in non USD exchange pairs), commonly refereed as sell and buy walls, to support the price within a narrow range of the 1 USD peg. The incentive to do so is the small commission between the market order and the 1 USD peg, usually <1%. Different users compete to be the closest price , so orders are filled with their walls and earn their profit, at the same time strengthening the 1 USD peg.

NuBits are the stable part of the **Nu Network**, the decentralized autonomous organization that started the project.

1.5.1 Notes

[1] NuBits does not have a central authority.

[2] NBT symbol is used by all exchanges accepting the currency. <https://nubits.com/exchanges/nubits-exchanges>

1.5.2 References

[1] <https://www.cryptocoinsnews.com/nubits-seeks-to-end-cryptocurrency-volatility-with-usd-peg/>

[2] Price history of NuBits (BTC price rounding adds +/-2%) <http://coinmarketcap.com/currencies/nubits/>

[3] https://www.reddit.com/r/peercoin/comments/3m4knf/nubits_becomes_the_first_decentralized_digital/

1.5.3 External links

- Official introductory video
- Official website for the Nu Network
- Official discussion about the Nu Network

1.6 Peercoin

Peercoin, also known as **PPCoin** or **PPC**, is a peer-to-peer cryptocurrency utilizing both proof-of-stake and proof-of-work systems.^{[4][5]}

Peercoin is based on an August 2012 paper which listed the authors as Scott Nadal and Sunny King.^[4] Sunny King, who also created Primecoin, is a pseudonym.^[6] Nadal's involvement had diminished by November 2013, leaving King as Peercoin's sole core developer.^[5]

Peercoin was inspired by bitcoin, and it shares much of the source code and technical implementation of bitcoin.^[7] The Peercoin source code is distributed under the MIT/X11 software license.^[8]

Peercoin is the fourth largest minable cryptocurrency by market capitalization. Peercoin has a market cap of \$30 million USD as of Jul 20, 2014.^[9] Unlike bitcoin, Namecoin, and Litecoin, Peercoin does not have a hard limit on the number of possible coins, but is designed to eventually attain an annual inflation rate of 1%. This feature, along with increased energy efficiency, aim to allow for greater long-term scalability.^[10]

1.6.1 Transactions

A peer-to-peer network handles Peercoin's transactions, balances and issuance through SHA-256, the proof-of-work scheme (Peercoins are issued when a small enough hash value is found, at which point the block of transactions is added to the shared block chain. The process of finding these hashes and creating blocks is called '**mining**').

Peercoins are currently traded for fiat currencies, bitcoins, and other cryptocurrencies, mostly on online exchanges. Reversible transactions (such as those with credit cards) are not normally used to buy Peercoins as Peercoin transactions are irreversible, so there is the danger of chargebacks.^[11]

Addresses

Payments in the Peercoin network are made to *addresses*, which are based on digital signatures. They are strings of 34 numbers and letters which always begin with the letter *P*. One can create as many addresses as needed without spending any Peercoins. It is quite common to use one address for one purpose only which makes it easy to see who actually sent the Peercoins.

Confirmations

Transactions are recorded in the Peercoin *blockchain* (a ledger held by most clients), a new block is added to the blockchain with a targeted time of 10 minutes (whenever a small enough hash value is found for the proof-of-work scheme), a transaction is usually considered complete after 6 blocks, or 60 minutes, though for smaller transactions, less than 6 blocks may be needed for adequate security.

1.6.2 Creation of New Coins

New coins can be created in two different ways; *mining* and *minting*. Mining uses the SHA-256 algorithm to directly secure the network. Minting rewards users proportionality to the coins that they hold (targeted at 1% annually). There are long term plans to reduce gradually the amount of mining and to rely more on minting. This is to create a fair distribution and could lead to an increase in the reward from minting.^[12]

1.6.3 Distinguishing features

Proof-of-stake

Peercoin's major distinguishing feature is that it uses a hybrid proof-of-stake/proof-of-work system. The proof-of-stake system was designed to address vulnerabilities that could occur in a pure proof-of-work system. With bitcoin, for example, there is a risk of attacks resulting from a monopoly on mining share. This is because rewards from mining are programmed to decline exponentially, which may decrease the incentive to mine.^[1] As miners decline, the likelihood of a monopoly increases, which leaves the network vulnerable to a 51% attack (a 51% attack is when a single entity possesses over half the mining share, which would allow this entity to theoretically double-spend a transaction involving their coins).^[13] With a proof-of-stake system, new coins are generated based on the holdings of individuals. In other words, someone holding 1% of the currency will generate 1% of all proof-of-stake coin blocks. This has the effect of making a monopoly more costly, and separates the risk of a monopoly from proof-of-work mining shares.^{[1][14]}

The proof-of-stake system also has other effects (listed below).^[1]

Proof-of-work

The whole network uses the SHA-256 Algorithm. For each 16 times increase in the network, the proof-of-work block reward is halved.

Energy efficiency

Peercoin's proof-of-stake system was developed to address the high energy consumption of bitcoin.^[1] For example, as of April 2013 the generation of bitcoins was using approximately \$150,000 USD per day in power consumption costs.^[15] The proof-of-stake method of generating coins requires very minimal energy consumption; it only requires the energy to run the client software on a computer, as opposed to running resource-intensive cryptographic hashing functions.^[1] During its early stages of growth, most Peercoins will be generated by proof-of-work like bitcoin, however over time proof-of-work will be phased out as proof-of-work difficulty increases and block rewards decrease.^[1] As Proof-of-stake becomes the primary source of coin generation, energy consumption (relative to market cap) decreases over time.^[1] As of January 2014, roughly 90% of new coins being generated are still from proof-of-work and the energy consumption of Peercoin uses roughly 30% of the energy consumption of bitcoin (scaling for market cap - in terms of value secured per GH/s).

Steady inflation

Peercoin is designed so that it will theoretically experience a steady 1% inflation per year, yielding an unlimited number of coins. This is a combined result of the proof-of-stake minting process, and scaling of mining difficulty with popularity.^[1] Although Peercoin technically has a cap of 2 billion coins, it is only for consistency checking, and the cap is unlikely to be reached for the foreseeable future. If the cap were to be reached, it could easily be raised, hence for all practical purposes Peercoin can be considered to have inflation of 1% per year, with a limitless money supply.^[1] This was partially designed to address the growing population.

Transaction fees

Peercoin is designed so that variable and optional transaction fees are removed in favor of a protocol defined transaction fee (currently 0.01 PPC/kB).^[1] The transaction fee is fixed at the protocol level and does not go to miners but is destroyed instead. This is intended to offset inflation by deflating the money supply and serves to self-regulate transaction volume, and stop network spam. One issue with a protocol defined transaction fee is that it does not evolve with the value of currency units, and requires a hardfork of the protocol to adjust transaction fees.

1.6.4 Other

Checkpointing

According to the original paper, Peercoin uses a centrally broadcast checkpoint mechanism.^[1] The paper cites Ben Laurie's argument that "Bitcoin has not completely solved the distributed consensus problem as the mechanism for checkpointing is not distributed." King notes that he attempted to design a distributed alternative, but ultimately concluded that a centralized solution was acceptable until a distributed solution became available.^[1]

1.6.5 See also

- Alternative currency
- Peer-to-peer computing
- Neucoin

1.6.6 References

- [1] King, S.; Nadal, S. (August 12, 2012). "PPCoin: Peer-to-peer crypto-currency with proof-of-stake" (PDF). *peercoin.net*. Retrieved 2013-12-23.
- [2] Bradbury, Danny. "Third largest cryptocurrency peercoin moves into spotlight with Vault of Satoshi deal". *Coindesk*. Retrieved 19 July 2014.
- [3] "Wary of Bitcoin? A guide to some other cryptocurrencies". *Wired.co.uk*. 2013-05-12.

- [4] “Peercoin News – AKA PPCoin or P2P Coin”. *CoinDesk*. Retrieved 23 February 2014.
- [5] Bradbury, Danny (7 November 2013). “Third largest cryptocurrency peercoin moves into spotlight with Vault of Satoshi deal”. *CoinDesk*. Retrieved 23 February 2014.
- [6] Popper, Nathaniel (24 November 2013). “In Bitcoin’s orbit: Rival virtual currencies vie for acceptance”. *The New York Times*. Retrieved 25 February 2014.
- [7] King, S. (2012). *What is ppcoin?* Retrieved from <https://github.com/ppcoin/ppcoin#what-is-ppcoin>
- [8] King, S. (2012). *PPCoin 0.3.0 BETA*. Retrieved from <https://github.com/ppcoin/ppcoin/blob/master/doc/README>
- [9] “Crypto-Currency Market Capitalizations”. Retrieved 2013-11-30.
- [10] Vega, Danny. “Peercoin: 5 Fast Facts You Need to Know”. *Heavy.com*. Heavy, Inc. Retrieved 20 July 2014.
- [11] “Bitcoin Isn’t the Only Cryptocurrency in Town”. *MIT Technology Review*. 2013-04-15.
- [12] <http://peercoin.net/mining>
- [13] Hern, Alex. “Bitcoin currency could have been destroyed by '51%' attack”. *The Guardian*. Guadian News & Media Ltd. Retrieved 2014-07-17.
- [14] “Wary of Bitcoin? A guide to some other cryptocurrencies”. *Arstechnica*. 2013-05-11.
- [15] “The Cost of a Bitcoin”. *TechCrunch*. 2013-04-13.

1.6.7 External links

- Official website
- Official Peercoin white paper

1.7 Titcoin

Titcoin (Ticker Symbol: TIT^[1]) is a type of digital currency called a **cryptocurrency** that uses **cryptography** on a decentralized **peer-to-peer** network to manage the issuance of new currency units while simultaneously processing transactions.^[2] Titcoin is a derivative of the **bitcoin** source code with key modifications to the software which greatly improve transaction speeds and network difficulty readjustments.^[3] Titcoin is exclusively designed for and marketed towards the **adult entertainment** industry to allow owners of the currency to pay for adult products and services without the fear of incriminating payment histories appearing on their **credit cards**.^{[4][5]}

Titcoin is notable for being the first **altcoin** fully recognized as a legitimate form of currency by a major industry trade organization. In 2015, Titcoin received two nominations at the 2015 **XBIZ Awards** ceremony which honors companies that play an essential part in the growth and success of adult entertainment.^[6] In 2016, Titcoin was nominated for a second year in a row as *Alternative Payment Services Company of the Year* at the 2016 **XBIZ Awards**.^[7]

1.7.1 History

Titcoin was originally founded by three cryptocurrency advocates from New York City: Edward Mansfield, Richard Allen and a third anonymous individual.^[8] The founders developed Titcoin for the adult entertainment industry as a cash **alternative payment** system for performing anonymous transactions.^{[9][10]} Titcoin allows consumers of adult entertainment to perform transactions without using any personally identifiable information.^{[11][12]} Titcoin also benefits adult businesses with zero **chargebacks** and freedom from dealing with traditional financial institutions.^{[13][14]}

On January 17, 2014, Titcoin was formally revealed to the cryptocurrency community with initial coin specifications and an official launch timeframe.^[15]

On June 21, 2014, the Titcoin wallet and source code was released with an initial soft launch for the cryptocurrency community followed by a hard launch for the public.^[16]

On August 26, 2014, the Titcoin wallet was successfully forked to support transaction times 10x faster than bitcoin and to enable real-time adjustments to the network difficulty level.^[17]

In September, 2014, former Wall Street stockbroker and Jordan Belfort protégé at Stratton Oakmont, Patrick McDonnell,^[18] joined the Titcoin development team as a business development advisor.^{[19][20]}

1.7.2 Specifications

Titcoin is a bitcoin clone that leverages the same SHA-256 set of cryptographic hash functions.^{[21][22]} The four key differences between Titcoin and bitcoin are the total number of coins to be issued, the total number of coins rewarded per block, the average block time, and the network difficulty retarget frequency.^[23]

1.7.3 Awards and Recognition

Titcoin has received several award nominations and ratings from notable organizations within the adult entertainment and cryptocurrency industries.

Adult Industry

- Alternative Payment Services Company of the Year (Finalist) - 2016 XBIZ Awards^[7]
- Alternative Payment Services Company of the Year (Finalist) - 2015 XBIZ Awards^[6]
- Innovative Web Product of the Year (Finalist) - 2015 XBIZ Awards^[6]

Cryptocurrency Industry

- 5 Plus+ POD Rating - Proof of Developer^[25]

1.7.4 Other adult cryptocurrencies

In addition to Titcoin, there are other lesser known cryptocurrencies that were similarly developed for the adult entertainment industry.

1.7.5 External links

- Official Titcoin Website

1.7.6 References


- [1] "TitCoin: A SHA256 Based Coin With A TIT In Adult Entertainment". *All Alt News*. Retrieved 5 October 2014.
- [2] Maguder, Natasha. "Explainer: How do cryptocurrencies work?". *CNN*. Retrieved 9 July 2014.
- [3] Moore, Lane. "Behind Titcoin, the New Anonymous Currency for Buying Porn". *Cosmopolitan Magazine*. Retrieved 30 October 2014.
- [4] Lynch, Gerald. "Titcoin is the Bitcoin for Porn". *Gizmodo UK*. Retrieved 23 June 2014.
- [5] Johnson, Bob. "'Titcoin' Aiming to Be Adult's Own Cryptocurrency". *XBIZ*. Retrieved 23 June 2014.
- [6] "Titcoin Receives Two Web & Tech XBIZ Nominations". *Payout Magazine*. Retrieved 18 November 2014.
- [7] Pedersen, Niels. "Titcoin and Coinsnap Nominated for Adult Entertainment Awards". *CryptoCoinsNews*. Retrieved 24 November 2015.
- [8] Mercier Voyer, Stephanie. "Titcoin Is a Brand New Cryptocurrency for Porn Purchases". *Vice Magazine*. Retrieved 18 June 2014.
- [9] Spitznagel, Eric. "Who Actually Pays for Porn Anymore? An Investigation". *Men's Health Magazine*. Retrieved 14 August 2014.
- [10] Weisman, Carrie. "Porn Gets Its Own Currency". *Design & Trend*. Retrieved 23 June 2014.

- [11] "Crypto-Currency for the Adult Industry Titcoin Founders Interviewed". *SoundCrave Magazine*. Retrieved 28 August 2014.
- [12] "Your complete A-Z guide to cryptocurrencies". *The Kernel*. Retrieved 11 January 2014.
- [13] Stryker, Kitty. "The adult industry's growing war over Titcoin". *The Daily Dot*. Retrieved 15 September 2014.
- [14] Beech, Richard. "Introducing Titcoin: The new currency only for adults". *The Daily Mirror*. Retrieved 29 October 2014.
- [15] "Titcoin (TIT) - Pre-Launch Announcement". *CryptoCoinTalk*. Retrieved 17 January 2014.
- [16] Chang, Lulu. "'Titcoin' Is A Bitcoin-Esque Currency For Porn, And Only Porn, And We Can't Even". *Bustle Magazine*. Retrieved 23 June 2014.
- [17] "Titcoin TIT Information [New Wallet Available | Fork to Occur Tue Aug 26 at 1200GMT]". *Crypto RSS*. Retrieved 26 August 2014.
- [18] Giles, Jeff. "Wolf of Wallstreet – Patrick McDonnell interview" *Major Mindjob*. Retrieved 29 January 2014.
- [19] Blue, Violet. "Why Is Wall Street Taking 'Titcoin' Seriously?". *Playboy Magazine*. Retrieved 24 October 2014.
- [20] "Patrick 'The Coyote of Wall Street' McDonnell Joins Titcoin". *AVN*. Retrieved 9 September 2014.
- [21] "TIT – Titcoin". *Altcoin.com*. Retrieved 22 June 2014.
- [22] "Meet porn's new cryptocurrency, Titcoin". *Times Live*. Retrieved 24 June 2014.
- [23] Buntinx, JP. "TitCoin - A Legit Cryptocurrency Contender In The Adult Entertainment Space?". *CryptoArticles*. Retrieved 15 September 2014.
- [24] "Titcoin TIT Information". *CryptoCoinTalk*. Retrieved 19 January 2014
- [25] "(TIT) Titcoin Proof of Developer Rating".
- [26] Soh, Stephanie. "Nine of the weirdest cryptocurrencies". *GQ Magazine*. Retrieved 8 August 2014.
- [27] "BitCoinTalk Launch Announcement for SexCoin". *BitCoinTalk*. Retrieved 28 May 2013.
- [28] "SexCoin Block Explorer".
- [29] "BitCoinTalk Launch Announcement for WankCoin". *BitCoinTalk*. Retrieved 26 May 2014.
- [30] "WankCoin Block Explorer".
- [31] "BitCoinTalk Launch Announcement for TitCoin". *BitCoinTalk*. Retrieved 21 June 2014.
- [32] "Titcoin Block Explorer".
- [33] "BitCoinTalk Launch Announcement for TittieCoin". *BitCoinTalk*. Retrieved 29 January 2014.
- [34] "TittieCoin Block Explorer".
- [35] "BitCoinTalk Launch Announcement for GroinCoin". *BitCoinTalk*. Retrieved 27 May 2014.
- [36] "GroinCoin Block Explorer".
- [37] "BitCoinTalk Launch Announcement for XXXCoin". *BitCoinTalk*. Retrieved 27 July 2014.
- [38] "XXXCoin Block Explorer".
- [39] "BitCoinTalk Launch Announcement for AnalCoin". *BitCoinTalk*. Retrieved 11 March 2015.
- [40] "AnalCoin Block Explorer".
- [41] "BitCoinTalk Launch Announcement for DickCoin". *BitCoinTalk*. Retrieved 26 April 2014.
- [42] "BitCoinTalk Launch Announcement for FellatioCoin". *BitCoinTalk*. Retrieved 15 January 2014.

Chapter 2

Script-based

2.1 Auroracoin

Auroracoin (code: AUR, symbol: ) is a peer-to-peer cryptocurrency launched in February 2014 as an Icelandic alternative to bitcoin and the Icelandic króna.^{[1][2][3]} Based on Litecoin with a script proof-of-work algorithm, its unknown creator or creators use the pseudonym Baldur Friggjar Óðinsson (or Odinsson).^{[1][2][3]} They stated that they planned to distribute half of auroracoins that would ever be created to all 330,000 people listed in Iceland's national ID database beginning on March 25, 2014, free of charge, coming out to 31.8 auroracoins per person.^{[1][3]}

Auroracoin was created as an alternative currency to address the government restrictions on Iceland's króna, in place since 2008, which severely restricts movement of the currency outside of the country.^[1] Iceland's Foreign Exchange Act also prohibits the foreign exchange of bitcoins from the country, according to a government minister.^[4] Auroracoin was the first of a number of country-based cryptocurrencies.^[5]

2.1.1 History

The pseudonym Baldur Friggjar Óðinsson is based on Norse mythology, referencing Baldur, his mother Frigg, and his father Odin.^[1]

Airdrop

By using the Kennitala national identification system to give away 50% of the total issuance of Auroracoins to the population of Iceland, a process dubbed the "airdrop", the developer hoped to bootstrap a network effect and introduce cryptocurrency to a national audience.^[6]

Phase 1 of the airdrop began on March 25, 2014, with 31.8 AUR being distributed to each claimant. With a USD value of \$12.11 per coin on March 24th, Icelanders were receiving the equivalent of \$385.^[7] Price quickly began to fall with the broad issuance of coins. Within one day of the Airdrop launch, approximately 281,000 coins had been distributed and price had dropped nearly 50% versus bitcoin.^[7] When phase one of the airdrop had completed on July 24, 2014 it was estimated that 1,126,674 AUR had been disbursed among 35,430 claimants, out of a total Iceland population of 323,002 (2013).^[8]

The second phase of the airdrop ran from July 25 to November 24, 2014. With the value of AUR having fallen dramatically against the krona the amount per claim was increased to 318 coins. About 5024 claims totalling almost 1.6 million coins were made.^[9]

The final phase of the airdrop took place from November 25, 2014 to March 24, 2015 with nearly 1.7 million coins being claimed by more than 2600 Icelanders. By this time the price had fallen so sharply that the payout had increased to 636 coins per recipient.^[10] On April 22, 2015 in accordance with the original airdrop plan, the 5,344,628 unclaimed pre-mined coins were verifiably 'burned' or made inaccessible by being sent to the address AURburnAURburnAURburnAURburn7eS4Rf.

Foundation

The Auroracoin Foundation was launched on March 29, 2015 to spearhead further technical development and promote the use of Auroracoin in Iceland. The Foundation was granted 1,000,000 AUR by the developer to help fund this work.^[11]

2.1.2 Controversy

Some Icelandic politicians have taken a negative view of Auroracoin. During a parliamentary debate on March 14, 2014, MP Pétur Blöndal, vice-chair of the Parliament's Economic Affairs and Trade Committee (EATC), emphasized that potential tax evasion through the use of Auroracoin could impact Iceland's economy.^{[12][13]} He also said that the public should realize that Auroracoin "is not a recognized currency since no-one backs the medium".^[12]

MP Frosti Sigurjónsson, a member of the ruling Progressive Party and Chairman of the EATC,^[12] suggested in a blog post on his website that there is evidence that Auroracoin is an illegal financial "scam".^{[13][14]}

Óðinsson said that "(parliament) can make it illegal to own or trade Auroracoin, however, they will never be able to control such a decentralized system, or stop Icelanders from using the currency, without turning Iceland into a police state."^[12]

Between its peak of around 0.1 BTC and March 30, 2014, Auroracoin's value fell to 0.004BTC.^[15] Auroracoin has begun to stabilize since the remaining pre-mined coins were burned on April 22, 2015.^[16]

2.1.3 References

- [1] Casey, Michael J. (March 5, 2014). "Auroracoin already third-biggest cryptocoin—and it's not even out yet". (Blog) *The Wall Street Journal*.
- [2] Rizzo, Pete (March 3, 2014). "Iceland's Auroracoin passes Litecoin, becomes third largest altcoin by market cap". *CoinDesk*.
- [3] Charlton, Alistair (March 4, 2014). "What is Auroracoin? Icelandic cryptocurrency passes Litecoin with \$1 billion valuation". *International Business Times*.
- [4] "Höftin stöðva viðskipti með Bitcoin [Controls suspend trading in Bitcoin]". *mbl.is* (in Icelandic) (Morgunblaðsins). December 19, 2013.
- [5] Gilbert, David (March 1, 2014). "Cryptocurrency News Round-Up: Aphroditecoin Woos Miners as Auroracoin Airdrop Nears". *International Business Times*.
- [6] "As Auroracoin "Airdrop" Approaches, What Does It Mean When A Nation Adopts A Cryptocurrency?". *Tech Crunch*. March 1, 2014.
- [7] Cawrey, Daniel (March 24, 2014). "Auroracoin Airdrop: Will Iceland Embrace a Digital National Currency?". *CoinDesk*.
- [8] <http://blockexplorer.auroracoin.eu/claims.html>
- [9] <http://blockexplorer.auroracoin.eu/claims.2.html>
- [10] <http://blockexplorer.auroracoin.eu/claims.3.html>
- [11] "General information about Auraráð in English". Auroracoin Foundation.
- [12] Gola, Yashu (March 15, 2014). "Auroracoin vs Icelandic Government". *Forex Minute*.
- [13] Cawrey, Daniel (March 14, 2014). "Icelandic Parliament Committee Holds Closed Session to Discuss Auroracoin". *CoinDesk*.
- [14] "Frosti Sigurjónsson" (in Icelandic). Frosti Sigurjónsson. March 7, 2014. Retrieved 2014-03-26. Ýmislegt bendir samt til þess að hér sé um að ræða peningasvindl og brot á lögum. Blog cited to provide original source of *CoinDesk's* translation.
- [15] <http://www.cryptocoinsnews.com/news/auroracoin-airdrop-flop/2014/03/30>
- [16] <http://explorer.auroracoin.eu/address/AURburnAURburnAURburnAURburn7eS4Rf>

2.1.4 External links

- Auroracoin Foundation official website
- Auroracoin community site

2.2 Coinye

Coinye, formerly **Coinye West**, is an abandoned^{[1][2][3]} script-based cryptocurrency that became embroiled in a trademark infringement lawsuit for using the American hip hop artist Kanye West as its mascot, despite West having no affiliation with the project.^{[4][5]} The project was abandoned by the original developers following West's filing of a trademark infringement lawsuit against them.^[6]

2.2.1 Release

Coinye was originally slated for release on January 11, 2014, but legal pressure prompted David P. McEnery Jr.^[7] and his development team to release the source code and mining software on January 7, a few days ahead of schedule.^[8] Early press materials promised a proper and fair release, with no pre-allocation of coins.^[9] However, later statements from the developers confirmed that approximately 0.37% of the maximum money supply of Coinye had been reserved for the creators of the coin before launch.^[10] The developers claimed that this was to cover unexpected legal and development costs.

2.2.2 Trademark infringement lawsuit

On January 6, 2014, Kanye West's lawyers sent the development team a **cease and desist** order on the basis that the then-unreleased currency constituted trademark infringement, unfair competition, cyberpiracy and dilution.^{[11][12]} In response to the legal threats, the development team changed the name of the currency from "Coinye West" to "Coinye" and moved to a new domain name.^[13] By January 10, 2014, the development team stated that they had removed all references to West but instead "to a half-man-half-fish hybrid," a nod to a *South Park* episode in which West fails to realize why people are jokingly calling him a "gay fish."^[14] These actions were not sufficient to appease West's legal team and a lawsuit was filed against the creators of the coin, prompting them to sell their Coinye holdings and leave the project.^[1]

2.2.3 Developer departure and community takeover

On January 14, 2014, a representative of Coinye announced on **Reddit** that "the developers basically dumped all their coins on the one exchange and left the scene."^{[11][15]} Coinye's official site was replaced with text reading "Coinye is dead. You win, Kanye."^[16] and the original website is now down.

Although the creators of the project closed down all official Coinye services and have distanced themselves from the parties they labeled "morons trying to revive this coin,"^[17] the peer-to-peer coin network is still operational and a group of volunteers has claimed that they will continue development on the coin.^[18] However, as of May 2015, no updates to the Coinye source code appear to have been released since the original developers' departure.^[19]

2.2.4 Decline of use

Coinye has been called "defunct" by numerous publications.^{[20][21][22][23][24]} Though the coin's peer-to-peer network is itself still functional, Coinye's global block difficulty fell from 78 to 1.012 between January 18, 2014^[25] and May 7, 2014,^[26] indicating that the network's total processing power fell by roughly 99% during that time.

2.2.5 External links

- <https://web.archive.org/web/20140517065834/http://coinyethecoin.com/> An archive of a web site about the cryptocurrency

2.2.6 References

- [1] Newton, Casey (14 January 2014). "Coinye developers say they're abandoning project as Kanye West escalates legal battle". *The Verge*. Retrieved 19 June 2014.
- [2] Marc, Schneider. "Kanye West Buries Coinye With Lawsuit Victory". *Billboard*. Retrieved 23 October 2015.
- [3] Rizzo, Pete. "Kanye West's Legal Team Take Down Spoof 'Coinye' Altcoin". *CoinDesk*. Retrieved 23 October 2015.
- [4] Yannick LeJacq (2 January 2014). "Oh Yeezus! Cryptocurrency gets hip with Kanye-inspired 'Coinye West'". NBC News. Archived from the original on 2014-01-02. Retrieved 19 June 2014.
- [5] Adam Gauntlett (3 January 2014). "Bitcoin Rival Coinye West To Launch This Month". *The Escapist*. Archived from the original on 2014-01-07. Retrieved 19 June 2014.
- [6] Winograd, David (14 January 2014). "Kanye Sues Coinye, and The Cryptocurrency's Creators Back Down". *TIME*. Archived from the original on 2014-02-02. Retrieved 19 June 2014.
- [7] <http://www.scribd.com/doc/224407868/DOCS-1320734-V1-Permanent-Injunction-on-Consent-David-McEneyr>
- [8] Danny Yadron (7 January 2014). "Kanye's Lawyer Moves to Block Coinye". *Digits*. *The Wall Street Journal*. Archived from the original on 2014-01-07. Retrieved 19 June 2014.
- [9] Clark, Liat (3 January 2014). "CoinYe West: a new cryptocurrency for the masses and ode to Kanye". *Wired*. Retrieved 19 June 2014.
- [10] Vega, Danny (8 January 2014). "Coinye West: 5 Fast Facts You Need to Know". *Heavy*. Retrieved 19 June 2014.
- [11] Rose, Brad (6 January 2014). "Infringement of KANYE WEST Mark and Other Violations" (PDF). Pryor Cashman LLP. Retrieved 19 June 2014.
- [12] Kyle Chayka (7 January 2014). "Bound 2 Happen: Kanye West Demands Coinye Programmers Shut Down the Digital Currency". *TIME*. Archived from the original on 2014-01-08. Retrieved 19 June 2014.
- [13] Danny Yadron (7 January 2014). "Kanye's Lawyer Moves to Block Coinye". *Digits*. *The Wall Street Journal*. Archived from the original on 2014-01-07. Retrieved 19 June 2014.
- [14] Adi Robertson (10 January 2014). "Coinye responds to Kanye complaint, says currency now based on 'half-man half-fish hybrid'". *The Verge*. Archived from the original on 2014-01-10. Retrieved 19 June 2014.
- [15] "Monday Updates". Retrieved 14 January 2014.
- [16] "coinyeco.in". Retrieved 14 January 2014.
- [17] Rizzo, Pete. "Kanye West's Legal Team Take Down Spoof 'Coinye' Altcoin". *CoinDesk*. Retrieved 17 January 2014.
- [18] "Interview: Coinye-initiatiefnemers". *fok.nl* (in Dutch). Retrieved 6 April 2014.
- [19] "coinyecoin software". Github. Retrieved 19 June 2014.
- [20] Higgins, Stan. "All Things Alt: Darkcoin Duels XC and the Demise of McDogecoin". *CoinDesk*. *CoinDesk*. Retrieved 3 June 2014.
- [21] Cox, Kate. "Bitcoin: What The Heck Is It, And How Does It Work?". *Consumerist*. Consumer Media LLC. Retrieved 3 June 2014.
- [22] O'Rourke, Patrick. "Kanye West kills the Coinye, a bitcoin-like cryptocurrency named after him". *canada.com*. Postmedia Network. Retrieved 3 June 2014.
- [23] McGovern, Kyle. "Coinye West Is Now Out of Print". *SPIN*. BUZZMEDIA. Retrieved 3 June 2014.
- [24] Burt, Chris. "Kanye West Sues Digital Currency Coinye, Alleged Hosting Provider AWS". *The Whir*. iNet Interactive. Retrieved 3 June 2014.
- [25] "The cryptocurrency who lived twice: Coinye is back [infographic]". *Bitcoin Examiner*. 18 January 2014. Retrieved 15 February 2014.
- [26] "Web Archive - CoinyeCoin Alt Explorer". *altexplorer.net*. Archived from the original on 2014-05-07. Retrieved 19 June 2014.

2.3 Dogecoin

Dogecoin (*/ˈdoʊʒkoɪn/ DOHZH-koyɪn*,^[2] code: **DOGE**, symbol: **Ð**^[1] and **D**) is a cryptocurrency featuring a likeness of the Shiba Inu dog from the "Doge" Internet meme as its logo.^{[3][4][5][6]} It was introduced on December 8, 2013.^[7] Started as a "joke currency" in late 2013, Dogecoin quickly developed its own online community and reached a capitalization of USD 60 million in January 2014;^[8] as of September 2015, it had a capitalization of USD 12.5 million.^[9]

Compared with other cryptocurrencies, Dogecoin has such fast initial coin production schedule: 100 billion coins have been in circulation by mid 2015 with an additional 5.256 billion coins every year thereafter. As of 30 June 2015, the 100 billionth Dogecoin has been mined.^[10] While there are few mainstream commercial applications, the currency has gained traction as an Internet tipping system, in which social media users grant Dogecoin tips to other users for providing interesting or noteworthy content.^[11] Many members of the Dogecoin community, as well as members of other cryptocurrency communities, use the phrase "To the moon!" to such describe the overall sentiment of the coin's rising value.^{[12][13][14]}

2.3.1 Overview and history



A Dogecoin paper wallet

Dogecoin was created by programmer Billy Markus from Portland, Oregon, who hoped to create a fun cryptocurrency that could reach a broader demographic than Bitcoin. In addition, he wanted to distance it from the controversial history behind bitcoin, mainly its association with the Silk Road online drug marketplace.^[15] At the same time, Jackson Palmer, a member of Adobe Systems' marketing department in Sydney, was encouraged on Twitter by a student at Front Range Community College to make the idea a reality.^[16]

After receiving several mentions on Twitter, Palmer purchased the domain dogecoin.com and added a splash screen, which featured the coin's logo and scattered Comic Sans text. Markus saw the site linked in an IRC chat room, and started efforts to create the currency after reaching out to Palmer. Markus based Dogecoin on the existing cryptocurrency, Luckycoin,^[17] which features a randomized reward that is received for mining a block, although this behavior was later changed to a static block reward in March 2014. In turn, Luckycoin is based on Litecoin,^[18] which also uses scrypt technology in its proof-of-work algorithm. The use of scrypt means that miners cannot use SHA-256 bitcoin mining equipment, and that dedicated FPGA and ASIC devices used for mining are complicated to create. Dogecoin was officially launched on December 8, 2013.^{[19][20]} The Dogecoin network was originally intended

to produce 100 billion Dogecoins, but later, it was announced that the Dogecoin network would produce infinite Dogecoins.^{[21][22][23]}

On December 19, 2013, Dogecoin jumped nearly 300 percent in value in 72 hours, rising from US\$0.00026 to \$0.00095,^[24] with a volume of billions of Dogecoins per day.^[25] This growth occurred during a time when bitcoin and many other cryptocurrencies were reeling from China's decision to forbid Chinese banks from investing Chinese Yuan into the bitcoin economy.^[18] Three days later, Dogecoin experienced its first major crash by dropping by 80% due to large mining pools seizing opportunity in exploiting the very little computing power required at the time to mine the coin.^[26]

On December 24, 2013, The Reserve Bank of India cautioned users of Dogecoin and other cryptocurrencies on the risks associated with them.^[27] On December 25, 2013, the first major theft attempt of Dogecoin occurred when millions of coins were stolen during a hacking attempt on the online wallet platform Dogewallet.^[28] The hacker gained access to the platform's filesystem and modified its send/receive page to send any and all coins to a static address.^{[29][30]} This incident spiked Tweets about Dogecoin making it the most mentioned altcoin on Twitter.^[31] To help those who lost funds on Dogewallet after its breach, the Dogecoin community started an initiative named "SaveDogemas" to help donate coins to those who lost them. Approximately one month later, enough money was donated to cover all of the coins that were lost.^[32] By January 2014, the trading volume of Dogecoin briefly surpassed that of bitcoin and all other crypto-currencies combined.^[33] As of 25 January 2015, Dogecoin has a market capitalization of USD 13.5 million.^[9]

2.3.2 Fundraising

2014 Winter Olympics

The Dogecoin community and foundation have encouraged fundraising for charities and other notable causes. On January 19, 2014, a fundraiser was established by the Dogecoin community to raise \$50,000 for the Jamaican Bobsled Team, which had qualified for, but could not afford to go to, the Sochi Winter Olympics. By the second day, \$30,000 worth of Dogecoin was donated,^[34] and the Dogecoin to bitcoin exchange rate rose by 50%.^{[35][36][37][38][39][40]} The Dogecoin community also raised funds for a second Sochi athlete Shiva Keshavan.^[41]

Doge4Water

Inspired by the Winter Olympics fundraiser and smaller charity fundraising successes, the Dogecoin Foundation, led by Eric Nakagawa, began collecting donations to build a well in the Tana river basin in Kenya in cooperation with Charity: Water. They set out to raise a total of 40,000,000 (\$30,000 at the time) Dogecoin before World Water Day (March 22). The campaign succeeded, collecting donations from more than 4,000 donors, including one anonymous benefactor who donated 14,000,000 Dogecoin (~ \$11,000) in what news media dubbed "the most valuable tweet in history".^[42]

NASCAR

On March 25, 2014, the Dogecoin community successfully raised 67.8 million Dogecoins (around \$55,000 at the time) in an effort to sponsor NASCAR driver Josh Wise. Wise ran with a Dogecoin/Reddit-sponsored paint scheme at the Aaron's 499 at Talladega Superspeedway.^[43] On May 4, 2014, Wise and his car were featured for nearly a minute, during which the race commentators discussed Dogecoin and the crowdfunding effort, while finishing 20th and narrowly avoiding multiple wrecks.^[44] On May 16, 2014, Wise won a spot at the Sprint All-Star Race through an online fan vote beating household name Danica Patrick, largely due to the efforts of the Dogecoin Reddit community. He finished the race in 15th, last car running.^{[45][46]} The following race in the Coca-Cola 600, Wise debuted a Dogecoin/Reddit.com helmet.^[47] Wise later announced he would run the car again at the Toyota/Save Mart 350^[48] as a thank-you gift to the community and the GEICO 500. He finished twenty-eighth in the race due in part to a refueling issue; he was in twelfth place after a gas-and-go pit stop, but the gas can did not engage long enough, resulting in a second pit stop that took him towards the back of the pack.^{[49][49]} The developer of the NASCAR '14 video game announced that they are looking into adding the Dogecoin car as a drivable car in an upcoming DLC.^{[46][50]}

2.3.3 Use and exchanges

Several online exchanges offer DOGE/BTC^[51] and DOGE/LTC^[52] trading. Three exchanges, Mengmengbi, Bter and BTC38, offer DOGE/CNY trading.^{[53][54]} On January 8, 2014, AltQuick.co was the first exchange to launch DOGE/USD exchange.^[55] On January 30, 2014, Canada-based exchange Vault of Satoshi also announced DOGE/USD and DOGE/CAD trading.^{[56][57]} On February 2014, Hong Kong-based exchange Asia Nexgen announced that they would support the trading of Dogecoins in all major currencies. China-based exchange BTC38 also added their support on the Dogecoin exchange, boosting the market capitalization over 24 hours.^{[58][59]} In the first day of trading, Dogecoin was the second-most traded currency on the platform, after BTC.^[60] Since September 2014 offers UK based exchange Yacuna DOGE trading in EUR and GBP.^[61]

On January 31, 2014, trading volume across the major exchanges was valued at \$1.05 million USD. The market cap was USD\$60 million. Three exchanges accounted for the majority of volume: Bter (60%), Cryptsy (23%), and Vircorex (10%). The most traded currency pairs were DOGE/BTC (50%), DOGE/CNY (44%) and DOGE/LTC (6%).^[62]

Trading physical, tangible items in exchange for DOGE takes place on online communities such as Reddit and Twitter.^{[63][64]} On December 23, 2013, Tristan Winters of the online journal *Bitcoin Magazine* discussed what was needed for Dogecoin to replace bitcoin.^[65]

The first Dogecoin ATM was demoed at Coinfest in Vancouver in February 2014.^[66] Two bitcoin ATMs supporting Dogecoins and other altcoins opened in Tijuana, Mexico on March 17, 2014.^[67]

Dogecoin has also been used to try sell a house,^[68] and has been used in the pornography^[69] and poker^[70] industries.

2.3.4 Transactions

See also: Bitcoin network

Like bitcoin and Litecoin, Dogecoin functions using public-key cryptography, in which a user generates a pair of cryptographic keys: one public and one private. Only the private key can decode information encrypted with the public key; therefore the keys' owner can distribute the public key openly without fear that anyone will be able to use it to gain access to the encrypted information. All Dogecoin addresses are public key hashes. Unlike bitcoin addresses, which are 27 to 33 characters long, Dogecoin addresses are a string of 34 numbers and letters (both upper and lower case), starting with the letter D. A public key is the Dogecoin address to which other users can send Dogecoins. A private key, however, allows full access to the Dogecoin wallet; it must be kept secret and secure. Dogecoin holds the record for most transactions per day for any cryptocurrency, peaking at 2.5 times more transactions than all other cryptocurrencies combined in December 2013.^[71]

2.3.5 Mining parameters

Dogecoin's implementation differs from Litecoin by several parameters. Dogecoin's block time is 1 minute as opposed to Litecoin's 2.5 minutes. The difficulty retarget time is once per block and the reward is fixed based on the block schedule listed below. However, when Dogecoin was first introduced, the difficulty retargeting was once every four hours, and the reward was a random number between 0 and a maximum defined by the block schedule. Under the system in which a random number of coins were distributed, rewards were calculated using a *Mersenne Twister pseudo-random number generator*.^[72] While the original implementation of Dogecoin meant for there to be a fixed number of coins per block from block 600,001 onwards only (providing 10,000 coins per block),^[7] the algorithms in Dogecoin were changed beginning from the 145,000th block so that a fixed reward was always given (providing 250,000 coins per block until block 200,001).^[73]

On March 12, 2014, version 1.6 of the Dogecoin client was announced. Along with allowing for there to be a fixed reward per block, the new client update also introduced a new difficulty algorithm called DigiShield. The main goal of the new difficulty algorithm, adopted from the DigiByte altcoin, was to prevent multipools from being able to mine (and thereby profit) off the coin, reducing the price of the coin drastically, along with forcing single-coin miners to deal with the rise in difficulty the pools left in their wake. Thanks to the algorithm's near-instant change in difficulty, any multipool entering the Dogecoin network will immediately leave, as the difficulty of mining will spike upwards severely, causing a drop in profitability and, ultimately, an absence of multipools.^[73]

Several cases of using employer or university computers to mine Dogecoin have been discovered.^{[74][75]}

2.3.6 Block schedule

2.3.7 Currency supply

Unlike deflationary cryptocurrencies (like bitcoin), there is no limit to how many Dogecoins can be produced. This puts Dogecoin in the same league as other inflationary coins. According to the current production schedule, approximately 98 billion coins have been released by February 2015, with block 600,000 mined on February 25. Thereafter, approximately 5.256 billion more coins will be produced per year, in perpetuity. This represents an inflation rate of 5.256% (in 2015), that will forever decrease though (e.g. in 2025 yearly inflation rate will be 3.4%, in 2035 2.5%, etc...). During December 2013 and January 2014, Dogecoin's developers discussed in public forums whether this should be changed,^{[22][84]} and, on February 2, 2014, Dogecoin founder Jackson Palmer announced that the supply of coins would remain uncapped.^[85]

2.3.8 References

- [1] "README.md". *Dogecoin Integration/Staging Tree* (Source code). February 5, 2014. Retrieved February 17, 2014.
- [2] Pronunciation of Dogecoin, wonder no more. on YouTube
- [3] Andrew Coutts (December 12, 2013). "Wow. Dogecoin is the most Internet thing to happen, ever.". *Digital Trends*. Retrieved December 2013.
- [4] Brittany Hillen (December 10, 2013). "Dogecoin digital currency takes on Bitcoin with a bit of meme flair". *Slashgear*. Retrieved December 2013.
- [5] "Dogecoin Order Book". *coinedup.com*. Retrieved 2013-12-19.
- [6] "Cryptocoin Market Capitalization". *coinmarketcap.com*. Retrieved 2013-12-19.
- [7] "Dogecoin - very currency many coin". Retrieved January 30, 2014.
- [8] Stephen Hutcheon. "The rise and rise of dogecoin, the internet's hottest cryptocurrency". *Sydney Morning Herald*. Fairfax Media. Retrieved April 5, 2014.
- [9] "Crypto-Currency Market Capitalizations | DogeCoin 30-Day Market Cap Graph". <http://coinmarketcap.com/currencies/dogecoin/>. Retrieved January 25, 2015. External link in |publisher= (help)
- [10] "Dogechain - The official dogecoin blockchain!". *Dogechain.info*. February 10, 2015. Retrieved February 10, 2015.
- [11] "The rise and rise of the Dogecoin and internet tipping culture". Australian Broadcasting Corporation. 24 January 2014. Retrieved 4 March 2015.
- [12] Andrew Coutts (December 19, 2013). "To the moon! Dogecoin fetches 300 percent jump in value in 24 hours". *Digital Trends*. Retrieved January 22, 2014.
- [13] Andrew Coutts (January 20, 2014). "Dogecoin users raise \$30,000 to send Jamaican bobsled team to Winter Olympics". *Digital Trends*. Retrieved January 22, 2014.
- [14] Derek Ross (December 31, 2013). "Much application. Such coin. Very Android. Dogecoin Wallet now available on Google Play". *Phandroid*. Retrieved January 22, 2014.
- [15] Patrick McGuire. "Such Weird: The Founders of Dogecoin See the Meme Currency's Tipping Point". *Motherboard*. Vice Media. Retrieved December 23, 2013.
- [16] Rob Wile (December 19, 2013). "What is Dogecoin?". *Business Insider*. Retrieved December 2013.
- [17] Dogecoin: 5 Fast Facts You Need to Know - *seattlepi.com*
- [18] David Gilbert (December 20, 2013). "What is Dogecoin? The Meme that Became the Hot New Virtual Currency.". *International Business Times*. Retrieved December 2013.
- [19] Ashe Schow (December 19, 2013). "Internet gold: Doge + Bitcoin = Dogecoin". *Washington Examiner*. Retrieved December 2013.
- [20] Dogecoin - <https://bitcointalk.org/index.php?topic=361813.msg3872986#msg3872986>
- [21] Danny Vega (December 9, 2013). "Dogecoin: 5 Fast Facts You Need to Know.". *Heavy.com*. Retrieved December 2013.

- [22] “Not actually capped at 100 billion?”.
- [23] Miles Klee (December 10, 2013). “With its own cryptocurrency, Doge has officially conquered 2013”. The Daily Dot. Retrieved December 2013.
- [24] Andrew Coutts (December 19, 2013). “To the moon! DogeCoin fetches 300 percent jump in value in 24 hours.”. Digital Trends. Retrieved December 2013.
- [25] Nekomata (December 25, 2013). “2014: The Year of Dogecoin? And where to buy DOGE.”. KonNeko.com. Retrieved January 2013.
- [26] Rob Wile (December 22, 2013). “Dogecoin Prices Crashed This Weekend”. Business Insider. Retrieved December 2013.
- [27] “RBI cautions users of Virtual Currencies against Risks” (PDF). December 24, 2013. Retrieved December 2013.
- [28] Ashley Feinberg (December 26, 2013). “Millions of Meme-Based Dogecoins Stolen on Christmas Day”. Gizmodo. Retrieved December 2013.
- [29] Catherine Shu (December 25, 2013). “Such Hack. Many Dogecoin. Very Disappear. So Gone. Wow.”. TechCrunch. Retrieved December 2013.
- [30] Salvador Rodriguez (December 26, 2013). “Millions of Dogecoins, currency based on a meme, are reported stolen”. Los Angeles Times. Retrieved December 2013.
- [31] Ofir Beigel (January 7, 2014). “Please, not another coin - which altcoins are worth taking a look at”. 99Bitcoins. Retrieved January 2014.
- [32] After Dogewallet Heist, Dogecoin Community Aims to Reimburse Victims | Digital Trends
- [33] John Russell (January 15, 2014). “Dogecoin is the Bitcoin world’s most traded currency, but it’s unlikely to be its most valuable”. The Next Web. Retrieved January 2014.
- [34] “Dogecoin Jamaican Bobsled Team Olympics”. Business Insider. January 20, 2014. Retrieved January 25, 2014.
- [35] Alex Hern. “It’s bobsleigh time: Jamaican team raises \$25,000 in Dogecoin | Technology”. theguardian.com. Retrieved January 25, 2014.
- [36] Rodriguez, Salvador (January 20, 2014). “Jamaican bobsled team boosts value of Dogecoin, currency based on meme”. latimes.com. Retrieved February 2, 2014.
- [37] “Dogecoin Jamaican Bobsled Team Olympics”. Business Insider. January 20, 2014. Retrieved February 2, 2014.
- [38] “Jamaican bobsled team raises \$30,000 in Dogecoin for trip to Sochi | The Rundown | PBS NewsHour”. PBS. Retrieved February 2, 2014.
- [39] Alex Hern. “It’s bobsleigh time: Jamaican team raises \$25,000 in Dogecoin | Technology”. theguardian.com. Retrieved February 2, 2014.
- [40] Marc Chandler (January 22, 2014). “Jamaican Bobsledding And Crypto Currencies”. Investing.com. Retrieved April 6, 2014.
- [41] Devin Coldewey (January 29, 2014). “Dogecoin cryptocurrency donors help send Indian athletes to Sochi”. NBC News.com. Retrieved February 2, 2014.
- [42] David Gilbert (March 17, 2014). “'Most Valuable Tweet in History' Donates \$11,000 Worth of Dogecoin to Kenyan Water Charity”. IB Times. Retrieved May 25, 2014.
- [43] Estrada, Chris (March 26, 2014). “NASCAR fans on Reddit use DogeCoin to sponsor Josh Wise”. NBC Sports. Retrieved March 26, 2014.
- [44] Stuckey, Daniel. “Talladega Shibe: The Dogecar’s NASCAR Highlights”. Retrieved May 6, 2014.
- [45] Mike Hembree (May 16, 2014). “Josh Wise wins fan vote, beats Danica Patrick”. USA Today. Retrieved May 18, 2014.
- [46] Owen S. Good (May 18, 2014). “Dogecoin, NASCAR’s strangest hood sponsor, will appear in its official video game”. Polygon. Retrieved May 18, 2014.
- [47] “Photo by joshwisercing”. *Josh Wise*. Instagram. May 25, 2014. Retrieved May 31, 2014.
- [48] Wilmoth, Josiah. “Josh Wise Announces He Will Drive the Dogecar Twice More in 2014”. Cryptocoins News. Retrieved June 4, 2014.

- [49] Josh Wise (/u/dogedriver) (October 20, 2014). "Talladega (:". Retrieved January 25, 2014.
- [50] Larry Frum (April 24, 2014). "Reddit, Dogecoin support NASCAR racer at Talladega". CNN. Retrieved May 18, 2014. Fans of the NASCAR '14 video game will also get the chance to race the Dogecoin car for themselves when it is added in an upcoming DLC pack. In fact, they have featured the scheme on a DLC pack that costs \$0.99 on the Xbox 360 and the Xbox One.
- [51] "Cryptocoin charts". Cryptocoincharts.info.
- [52] "Cryptocoin charts". Cryptocoincharts.info.
- [53] "Bitcoin and Crypto-currency Exchange Platform". Bter.com. Retrieved January 25, 2014.
- [54] "Mengmengbi and Crypto-currency Exchange Platform". Bter.com. Retrieved April 11, 2014.
- [55] Pick, Leon (January 28, 2014). "AltQuick.co becomes man's 2nd best friend: allows dogecoin buying with USD". *Digital Currency Magnates*.
- [56] Bradbury, Danny (January 29, 2014). "Vault of Satoshi rolls out new altcoin support". *Coindesk*.
- [57] "Vault of Satoshi adds new alt-coins and a CAD order book, coin-to-coin trading imminent" (Press release). Global Cryptocurrency Solutions via PRWeb.com. January 30, 2014. Retrieved January 31, 2014.
- [58] Rizzo, Pete (February 13, 2014). "Asian exchange additions drive dogecoin price surge". *Coindesk*.
- [59] Charlton, Alistair (February 13, 2014). "Cryptocurrency news round-up: London bitcoin ATM update and dogecoin joins two exchanges". *International Business Times*.
- [60] Pick, Leon (January 30, 2014). "Dogecoin and quarkcoin hot, other altcoins not, on first day Vault of Satoshi trading". *Digital Currency Magnates*. Retrieved January 31, 2014.
- [61] "How to Buy Bitcoin in the UK". *Coindesk*. 2014.
- [62] "DOGE charts and information". Cryptocoincharts.info. Retrieved January 31, 2014.
- [63] Nathan Ingraham (December 16, 2013). "Bitcoin is so 2013: Dogecoin is the new cryptocurrency on the block". The Verge. Retrieved December 2013.
- [64] J. Duaine Hahn (December 16, 2013). "Move Over Bitcoin: Dogecoin is Here". Complex Tech. Retrieved December 2013.
- [65] Will Dogecoin Replace Bitcoin? – Bitcoin Magazine
- [66] Hajdarbegovic, Nermin (February 18, 2014). "DIY Dogecoin ATM demos at CoinFest Vancouver". *Coindesk*. Retrieved March 17, 2014.
- [67] Hajdarbegovic, Nermin (March 17, 2014). "Mexico's first bitcoin ATMs will also deal in altcoins". *Coindesk*. Retrieved March 17, 2014.
- [68] Imam, Jareen. "Man selling home for \$135,000 in Dogecoins". CNN. Retrieved March 17, 2014.
- [69] "Fox on Reddit: Porn star looks to accept virtual currency Dogecoin". *FoxNews.com*. February 27, 2014. Retrieved March 17, 2014.
- [70] "Dogecoin and Poker: A match made in heaven?". Dogecoin Poker Blog. April 25, 2014.
- [71] <https://bitinfocharts.com/comparison/transactions-btc-ltc-doge.html>
- [72] "Dogecoin C++ code for generating block rewards".
- [73] "Dogecoin 1.6 - It's ready. All you need to know inside.". Reddit. Retrieved March 12, 2014.
- [74] Hutchinson, Lee (February 21, 2014). "Harvard supercomputing cluster hijacked to produce dumb cryptocurrency". *Ars technica* (Condé Nast.). Retrieved June 13, 2014.
- [75] Hern, Alex (March 4, 2014). "Student uses university computers to mine Dogecoin". Guardian.com. Retrieved June 13, 2014.
- [76] "Dogechain - The official Dogecoin blockchain!". *Blockchain Record for Block 1*. Retrieved January 30, 2014.
- [77] "Dogechain - The official Dogecoin blockchain!". *Blockchain Record for Block 100000*.

- [78] “Dogechain - the official Dogecoin blockchain!”. *Blockchain Record for Block 145000*. Retrieved March 17, 2014.
- [79] “Dogechain - the official Dogecoin blockchain!”. *Blockchain Record for Block 200000*. Retrieved April 28, 2014.
- [80] “Dogechain - the official Dogecoin blockchain!”. *Blockchain Record for Block 300000*. Retrieved July 19, 2014.
- [81] “Dogechain - the official Dogecoin blockchain!”. *Blockchain Record for Block 400000*. Retrieved October 6, 2014.
- [82] “Dogechain - the official Dogecoin blockchain!”. *Blockchain Record for Block 500000*. Retrieved February 27, 2015.
- [83] “Dogechain - the official Dogecoin blockchain!”. *Blockchain Record for Block 600000*. Retrieved February 27, 2015.
- [84] “You should all be aware of this: Current algorithm increases the supply by at least 5,256,000 D yearly for eternity. The devs plan to make the supply fixed”. Reddit. Retrieved January 30, 2014.
- [85] “Dogecoin to allow annual inflation of 5 billion coins each year, forever”. Ars Technica. Retrieved February 4, 2014.

2.3.9 External links

- Official website

2.4 Litecoin

Litecoin (**LTC** or **Ł**^[1]) is a peer-to-peer cryptocurrency and open source software project released under the MIT/X11 license.^[2] Inspired by and technically nearly identical to bitcoin (BTC), Litecoin creation and transfer is based on an open source protocol and is not managed by any central authority.^{[2][3]}

After Bitcoin, Litecoin is the second-largest true cryptocurrency by market capitalization.^[4]

2.4.1 History

Litecoin was released via an open-source client on GitHub on October 7, 2011 by Charles Lee, a former Google employee.^[5] It was a fork of the Bitcoin-Qt client, differing primarily by having a decreased block generation time, increased maximum number of coins, different hashing algorithm (scrypt, instead of SHA-256^[6]), and a slightly modified GUI.

During the month of November 2013, the aggregate value of Litecoin experienced massive growth which included a 100% leap within 24 hours.^[7]

Litecoin reached a \$1 billion marketcap in November 2013.^[8] As of August 2015, its market capitalization is US\$181,542,352 with the price at \$4 levels.^[9]

2.4.2 Development

Litecoin version 0.8.5.1 was released in November 2013. The release included fixes for vulnerabilities and added enhanced security to the Litecoin network.

The Litecoin developer team released version 0.8.6.1 in early December 2013. The new version offered a 20x reduction in transaction fees, along with other security and performance improvements in the client and network. The source code and binaries were released early to people in the “#litecoin” IRC channel, on the official Litecoin forums, and on Reddit, with information for power users to add a Litecoin supernode to the configuration file, while the main site was to be updated after enough of the network was running the new version. This release method was used to ensure that the low fee transactions from version 0.8.6.1 clients would not be delayed by clients running older versions.

In April 2014, a new version of Litecoin was released, version 0.8.7.1, which fixed some minor issues along with an important fix related to the Heartbleed security bug.

2.4.3 Differences from Bitcoin

Litecoin offers three key differences from Bitcoin.

- The Litecoin Network aims to process a block every 2.5 minutes, rather than Bitcoin's 10 minutes, which its developers claim allows for faster transaction confirmation.^{[2][10]} A drawback is a higher probability of orphaned blocks. Advantages can include greater resistance to a double spending attack over the same period as bitcoin. However, total work done is a consideration. For example, if the Litecoin Network has comparatively ten times less computing work done per block than the bitcoin network, the bitcoin confirmation is around ten times harder to reverse, even though the Litecoin Network is likely to add confirmation blocks at a rate four times faster.
- Litecoin uses *script* in its *proof-of-work* algorithm, a sequential memory-hard function requiring asymptotically more memory than an algorithm which is not memory-hard.^[11]
- The Litecoin Network will produce 84 million Litecoins, or four times as many currency units as will be issued by the Bitcoin Network.

The original intended purpose of using Script was to allow miners to mine both Bitcoin and Litecoin at the same time.^[5] The choice to use script was also partially to avoid giving advantage to *video card (GPU)*, *FPGA* and *ASIC miners* over *CPU* miners; although Charlie Lee has never publicly agreed with this opinion.

Due to Litecoin's use of the script algorithm, FPGA and ASIC devices made for mining Litecoin are more complicated to create and more expensive to produce than they are for bitcoin, which uses SHA-256.^[12] This is widely due to the Script hashing scheme being more memory intensive; increasing memory requirements for ASICs and FPGAs. However, as of December 2015, ASIC miners are widely available and the primary method of mining Litecoin.

2.4.4 Transactions

A peer-to-peer network similar to bitcoin's handles Litecoin's transactions, balances and issuance through script, the *proof-of-work* scheme (Litecoins are issued when a small enough hash value is found, at which point a block is created, the process of finding these hashes and creating blocks is called mining). The issuing rate forms a *geometric series*, and the rate halves every 840,000 blocks, roughly every four years, reaching a final total of 84 million LTC.

Litecoins are currently traded primarily for both *fiat currencies* and other cryptocurrencies, mostly on online *exchanges*. To avoid the danger of *chargebacks*, reversible transactions, such as those with *credit cards*, are not normally used to buy litecoins as Litecoin transactions are irreversible.

Addresses

Payments in the Litecoin network are made to *addresses*, which are Base58-encoded hashes of users' *public keys*. They are strings of 33 numbers and letters which always begin with the letter *L*.

Confirmations

Litecoin transactions are recorded in the Litecoin *blockchain* (a *ledger* held by most clients). A new block is added to the blockchain roughly every 2.5 minutes (whenever a small enough hash value is found for the *proof-of-work* scheme). A transaction is usually considered complete after six blocks, or 15 minutes, though for smaller transactions, fewer than six blocks may be needed for adequate security.

2.4.5 Wallets

The most common Wallet available today is "Litecoin Core" for Linux, Windows and Mac OS. Litecoin Core is an offline wallet based on the Bitcoin Core wallet.

On January 19, 2014, the Litecoin Android wallet was released. This new release replaces the old Android client which contained major security issues.

A new Litecoin Electrum client — a lightweight wallet for Litecoin — was released for beta testing on April 10, 2014. As with other Litecoin Dev projects, the client is based on the bitcoin source and the Litecoin developers fix issues upstream in order to make it easier to keep the Litecoin version updated. As with the Litecoin Android wallet, this new version of Electrum for Litecoin replaces the old and unsupported version created in the first year of Litecoin's release.

2.4.6 Exchanges

As of February 2015 there are many [exchanges](#) that deal with Litecoin. Although some exchanges allow only trading between litecoins and bitcoins, many exchanges provide trading between litecoins and US dollars (247exchange, Bitfinex, BTC-e, OKCoin, BitBay), Euros (Kraken, Yacuna), and Chinese Yuan (Huobi, BTC China, OKCoin).^[13]

2.4.7 See also

- Bitcoin
- Crypto-anarchism
- Private currency

2.4.8 References

- [1] "Litecoin charts". ltc-charts.com. Retrieved 2014-01-19.
- [2] "Litecoin.org". litecoin.org. Retrieved 2014-01-19.
- [3] Satoshi, Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). Bitcoin.org. Retrieved 24 April 2013.
- [4] "Crypto-Currency Market Capitalizations". coinmarketcap.com. Retrieved 2015-02-08.
- [5] Coblee (user id) (2011-10-09). "[ANN] Litecoin — a lite version of Bitcoin. Launched!". Post on Bitcointalk.org internet forum. Retrieved 2014-05-03. Using Scrypt allows one to mine Litecoin while also mining Bitcoin.
- [6] "Block hashing algorithm".
- [7] Charlton, Alistair (2013-11-28). "Litecoin value leaps 100% in a day as market cap passes \$1bn". *International Business Times, UK Edition*. Retrieved 2013-12-16.
- [8] Cohen, Reuven (2013-11-28). "Crypto-currency bubble continues: Litecoin surpasses billion dollar market capitalization". *Forbes*. Retrieved 2014-01-19.
- [9] "Litecoin Charts - Litecoin Cryptocurrency Blockchain Explorer". Retrieved 4 August 2015.
- [10] Steadman, Ian (2013-05-11). "Wary of Bitcoin? A guide to some other cryptocurrencies". *Ars Technica*. Retrieved 2014-01-19.
- [11] Percival, Colin. "Stronger key derivation via sequential memory-hard functions" (PDF). Self-published. Retrieved 2013-04-24.
- [12] Coventry, Alex (2012-04-25). "Nooshare: A decentralized ledger of shared computational resources" (PDF). Self-published. Retrieved 2012-09-21. These hash functions can be tuned to require rapid access a very large memory space, making them particularly hard to optimize to specialized massively parallel hardware.
- [13] "Bitfinex LTCUSD". *Cryptowat.ch*. Retrieved 9 February 2015.

2.4.9 External links

- Official website

2.5 PotCoin

PotCoin (code: **POT**^[21]) is a peer-to-peer cryptocurrency which exists with the aim of becoming the standard form of payment for the legalized cannabis industry.^[2] PotCoin is an open source software project released under the MIT/X11 license and was technically nearly identical to Litecoin until August 23, 2015, when PotCoin changed to POSV similar to Reddcoin. PotCoin is not managed by any central authority and provides a decentralised solution for the transfer of value. As of August 2014, PotCoin has received mainstream media coverage from agencies such as Fox Business,^[3] Vice^[4] and TechCrunch.^[5]

2.5.1 History

PotCoin was released on January 21, 2014, via GitHub by three entrepreneurs from Montreal, Canada, who hoped to create a cryptocurrency that would be adopted by the legal cannabis industry across the world.^[2] A week after launch, PotCoin had enough interest to merit multiple mining pools and on January 30, was added to a newly launched cryptocurrency exchange named Cryptorush allowing trading between Bitcoin and PotCoin.^[6] During February and March 2014, PotCoin gained mainstream media attention due to the large community and expanding development team. On February 17, Chronic Star Medical, a supplier of cannabis foods, was the first merchant to announce they would be accepting PotCoin as a form of payment.^[7] By the end of March, PotCoin was added to three cryptocurrency exchanges that account for the largest trade volume to this date^[8] and the development team had announced that they had secured their first seed-round investment.^[9]

On April 9, 2014, the PotCoin development team revealed their identities for the first time when co-founders and developers Joel Yaffe and Nick Iversen delivered a talk about PotCoin at the New York Cryptocurrency Convention.^[10] The team also announced that they would be present in Denver on April 20 for the 420 counterculture holiday. On April 19, 2014, PotCoin witnessed a dramatic rise in price, taking its market capitalization over 1 million USD^[11] for the first time, fuelled by excitement around the April 20th counterculture holiday. On April 20, PotCoin experienced its first major crash with the value halving in one day due to speculation by investors.

The market capitalisation then sunk to a low of \$244,000 on May 22, 2014. On May 27, PotCoin ATMs were made available for use in two River Rock Wellness dispensaries in Colorado which was regarded as a major milestone and helped overturn the downtrend in price leading to an all-time high market capitalization of \$1,860,000 on July 1.^[11]

Early 2015 showed dark times for Potcoin. The original development team broke apart and left for various reasons. At this point the community tried to rally Potcoin away from death as a community-driven coin. PotLabs, a group of people who had helped to develop many things for Potcoin in the early years, took charge of the push to keep Potcoin alive and moving forward.

On August 23, 2015, Potlabs released an update for Potcoin, one that was very anticipated. With this Potcoin began its move to the POSV algorithm. Over the next few weeks there were some issues with the network getting up to speed. Many cryptocurrency exchanges also froze their Potcoin wallets waiting to see what would happen. Within a few weeks the network began to get up to speed and when exchanges were notified they began to unfreeze their wallets allowing normal transactions to resume.

2.5.2 Overview and specification

Much like Bitcoin, PotCoin is based on a public ledger known as a block chain.^[12] PotCoin was originally a fork of Litecoin-QT but with key differences including a shorter block generation time, a quicker halving schedule and an increased maximum number of coins.^[13] Before PotCoin was publicly released, 55 blocks were mined for checkpoints. The initial block reward (the number of coins rewarded for solving a block whilst mining) was set a 420 PotCoins but on June 1, 2014, the block reward was halved and currently stands at 210 PotCoins.^[14] Mining can be performed by hardware including CPUs, GPUs and more commonly script ASICs. On August 23, Potcoin changed mining algorithms from Script to POSV, a proof of stake algorithm designed to reward not only the ownership of coins but also transactions.

2.5.3 Usage

Wallets

A PotCoin wallet is used to store, send and receive PotCoin and is the equivalent of a physical wallet for transactions. Addresses are generated with a private key which can be used to redeem wallet contents and a public key which must be used by the payer to send PotCoins to the payee's wallet. The public key is a unique identifier of 26–34 alphanumeric characters and is commonly known as one's address. PotCoin wallets can be desktop software or mobile application or can be hosted on the Internet.

PotCoin-Qt is an open-source PotCoin client that can be used as a desktop client for regular payments or as a server utility for merchants and other payment services. The PotCoin-Qt client is a fork of Litecoin-Qt and binaries are available for Windows, Mac and Linux. Electrum-Pot is an open-source wallet that can be used as an alternative to PotCoin-Qt. The Electrum wallet differs in that a remote server is used and so an end-user does not need to download the blockchain. A single wallet can also be used on numerous devices by using a secret seed.

There are numerous online services dedicated to hosting PotCoin wallets allowing users to store PotCoins remotely and access through a **smartphone**. Many online services host wallets on their servers enabling users to deposit and withdraw a balance from their website.

The use of physical items to store a private key is known as cold storage with a common example being paper wallets.^[15] To redeem and send PotCoins held in cold storage, the private key must be imported into an electronic wallet.

Buying and selling

PotCoin can be traded online at numerous **digital currency exchanges** for **Bitcoin**, **Litecoin**, **Dogecoin** and **Darkcoin**. As of November 8, 2014, Cryptsy accounts for 91.7% of the trading volume, Bittrex 8.12% and seven other exchanges contributing towards the other 0.18% of trading volume.^[16] There are also sites that facilitate private and local trades with LocalPot being a notable example.^[17]

Spending

As of November 8, 2014, there are 44 merchants accepting PotCoin as a payment method for products or services.^[18]

2.5.4 Charitable fundraising

Snoop Youth Football League

On February 16, 2014, the PotCoin community paid \$500 to Snoop Youth Football League, a charity set up by Snoop Dogg. The Snoop Youth Football League is a 501c3 non-profit organization that gives inner-city children between ages 5 and 13 the chance to participate in youth football and cheer.^[19] It took the community two days to raise the required 55,000 PotCoins.^[20] A video message was posted by Snoop Dogg thanking Nick Iverson, a PotCoin developer, for the contribution and bonus prizes were sent to a number of community members.^[21]

Cannabis Health Service

On June 6, 2014, 18500 PotCoins were paid to the Cannabis Health Service, an organisation based in the UK, after a community on PotFunder.^[22] The Cannabis Health Service was founded by Colin Davies, a prominent activist with the aim of helping patients who believe, or have found, cannabis to be beneficial for the treatment of their illnesses.^[23]

FRAXA Research Foundation

On July 8, 2014, a check for US\$2000 was presented to the FRAXA Research Foundation after a community fundraising initiative through PotFunder.^[24] The fund-raising campaign was pioneered by PotCoin team member Russell Thomas who has a son that suffers from **Fragile X syndrome** (a form of mental retardation and the leading known cause of autism^[25]). FRAXA is a 501c3 non-profit organization whose mission is to find effective treatments and ultimately a cure for Fragile X.^[26]

Healthy Hopes

On August 2, 2014, 32578 PotCoins were paid to Healthy Hopes after a campaign on PotFunder.^[27] Healthy Hopes are a charity whose mission is to provide safe access to medical cannabis to seriously and chronically ill patients who have no hopes of legally obtaining the medicine they need where they live.^[28]

2.5.5 References

- [1] "PotFunder". potfunder.com. Retrieved 2014-08-06.
- [2] "[ANN] [POT] PotCoin Launches Today 01/21 @ 4:20". bitcointalk.org.
- [3] "DopeCoin, PotCoin Want to Solve Marijuana's Banking Problems". <http://smallbusiness.foxbusiness.com/>. Retrieved 6 August 2014.
- [4] "Stoners Now Have Their Own Cryptocurrency: PotCoin". <https://news.vice.com>. VICE. Retrieved 6 August 2014. External link in lwebsite= (help)
- [5] "Potcoin, A New Cryptocurrency To Help Ease The War On Drugs". <http://techcrunch.com/>. Retrieved 6 August 2014.
- [6] "[ANN] [POT] PotCoin Launches Today 01/21 @ 4:20". bitcointalk.org.
- [7] "Chronic Star Medical accepting PotCoin: "We believe in its core idea"". <http://highonpotcoin.info/>.
- [8] "PotCoin Markets". <http://coinmarketcap.com/>.
- [9] "PotCoin devs secure first round of investment to further the coin". <http://highonpotcoin.info/>.
- [10] "PotCoin @ CryptoCurrency Convention NYC 4/9/14 - Nick Iversen". *YouTube*.
- [11] "Crypto-Currency Market Capitalizations". <http://coinmarketcap.com/>.
- [12] "Github potcoin". *GitHub*.
- [13] "Potcoin (POT)". coingecko.com. Retrieved 6 August 2014.
- [14] "PotCoin halving schedule announced". <http://highonpotcoin.info/>.
- [15] "Paper wallet".
- [16] "PotCoin Markets". coinmarketcap.com.
- [17] "LocalPot.com - Potcoin Statistics". *Local Pot*.
- [18] "Merchants Accepting PotCoin". *PotCoin*.
- [19] "Win an internship for a day with Snoop".
- [20] "Snoop's Youth Football Charity, Success!". *PotCoin Subreddit*.
- [21] "Snoop Dogg thanks Nick Iverson". *Facebook*.
- [22] "Cannabis Health Centre Campaign". *PotFunder*.
- [23] "Cannabis Health Service C.H.S".
- [24] "Fragile-X-Syndrome campaign". *PotFunder*.
- [25] "FRAXA Research Foundation".
- [26] "About FRAXA".
- [27] "Healthy Hopes Campaign". *PotFunder*.
- [28] "Healthy Hopes".

Chapter 3

CryptoNote-based

3.1 CryptoNote

CryptoNote is an application layer protocol that powers several decentralized privacy oriented digital currencies. Conceptually, it is an evolution of ideas behind bitcoin: both are similar in some ways yet different in many others.^{[1][2]}

The main difference between the two technologies is that bitcoin (and most digital currencies) is less opaque than CryptoNote-based currencies due to the later's **blockchain** being almost anonymous, contrary to non-Cryptonote blockchains.^{[3][4]} CryptoNote currencies use a distributed public ledger that records all balances and transactions of its in-built currency like bitcoin. Unlike bitcoin, CryptoNote's transactions cannot be followed through the blockchain in a way that reveals who sent or received coins. The approximate amount of a transaction can be known, but the origin, destination, or actual amount cannot be learned. The only information available is that the actual amount was lower than the displayed amount. The only people with access to the whole set of data about a transaction are the sender or receiver of the transaction and the person who possesses one or both secret keys.

Another significant difference is **hash-based proof-of-work** algorithm. Bitcoin uses **SHA256**, which is CPU-bound function. That means that participants (miners) are only limited by their calculation speeds, and it is relatively cheap to create an **application-specific integrated circuit (ASIC)** device, which will surpass an ordinary computer in hashes per unit of money.^[5] CryptoNote uses **memory bound function CryptoNight**, which cannot be easily pipelined.^[6]

CryptoNote code was not **forked** from bitcoin's, so it also has other different inner algorithms, like recalculating new difficulty level or new block size.^[6]

3.1.1 Origins

CryptoNote technology was first described in a whitepaper *CryptoNote v 1.0*.^[7] An updated version has been released under the name *CryptoNote v 2.0*.^[6] later. The Bytecoin cryptocurrency was the first one where the underlying cryptographic protocol has been implemented. CryptoNote was at first developed in Java for faster launch, and then re-written in C++ in 2013.^[8]

CryptoNote is based on many early works and protocols and takes into consideration several issues raised formerly. Below is the list of most important papers and events influenced CryptoNote:^[9]

- 1983 – Blind signatures described by David Chaum;^[10]
- 1997 – HashCash (an instance of a proof-of-work system) invented by Adam Back;
- 2001 – Ron Rivest, Adi Shamir, and Yael Tauman proposed ring signatures to the cryptographic community;^[11]
- 2004 – Patrick P. Tsang and Victor K. proposed using the ring signature system for voting and electronic cash;^[12]
- 2008 – Bitcoin whitepaper published by Satoshi Nakamoto;^[13]
- 2010 - 2012 – Bitcoin Traceability Issue Discussion Gains Steam;^[14]

- 2011 – An Analysis of Anonymity in the Bitcoin System, Fergal Reid and Martin Harrigwere;^[15]
- 2012 – Destination Address Anonymity in Bitcoin (one-time addresses in CryptoNote).^[16]

3.1.2 Anonymous transactions and ring signatures



The changes in the results of blockchain analysis after implementing the ring signatures.

Like bitcoin, CryptoNote currencies use a **public address** consisting of **pseudorandom** numbers and letters that is derived from user's **public keys**. Addresses serve as public IDs of the users. However, unlike bitcoin, CryptoNote transactions hide the connection between the sender's and the receiver's addresses.

Sender privacy

To prevent sender identification, CryptoNote groups the sender's public key with several other keys (more precisely, it groups the sender's output with several other's outputs), making it impossible to tell who actually sent the transaction.^[17] If **ring signatures** are used, all possible senders referenced in the transaction are equiprobable and there is no way to determine the exact **private key** used while signing.^[18] This approach does not require dedicated **master nodes** for mixing coins and does not need other users to actively participate in transaction generation (see CoinJoin^[19]). It still assures the network that the original sender has the funds in his or her account to send the transaction like an ordinary signature scheme does. Instead of proving in **zero knowledge** manner the fact "I possess the private key which corresponds to this particular public key" the signer proves "I possess *at least one* of the private keys which correspond to this set of public keys".

Receiver privacy

On the receiver's end, the technology generates a new public key for each money transfer,^[20] even for the same sender and receiver. With sender's random data and receiver public address it is possible to create a pair of unique private and public keys via **Diffie-Hellman protocol**. Sender generates one-time **ephemeral key** for each transfer and only the receiver can recover the corresponding private key (to redeem the funds). No third party can determine if two different transactions were sent to the same recipient.

3.1.3 Double spending protection

Anonymous transactions have a potential problem. Bitcoin and similar currencies use a public ledger to verify that each person sending funds actually has such funds in their account and have not sent it to another user previously. Since CryptoNote currencies are anonymous, the network must confirm the validity of transactions in another way.

CryptoNote solved this problem^[21] by using more sophisticated scheme instead of usual ring signature: **traceable ring signature**. The algorithm originally proposed by Fujisaki and Suzuki in 2007^[22] allows to trace the sender of two different messages if they contain the same *tag* and signed by the same private key.

CryptoNote authors slightly simplified the scheme, replacing *tag* with *key image* and discarding the traceability property. They called their algorithm *one-time ring signature*, “stressing the user’s capability to produce only one valid signature under his private key”.^[6] Two different signatures under the same key (a double spend attempt) can be easily linked together, and only one will be stored in the blockchain.

The key idea is in using the image of the private key in signing/verification formulas. These are not actual images that would contribute greatly to blockchain bloat, but rather a number, which corresponds to each private key one-to-one (deterministically derived from it by the cryptographic hash function). The key image cannot be used to derive the private key and public address, but since every key image spent is stored in the blockchain, the network will block any duplicates. Likewise, any attempt to create a key image would not fit into the mathematical formula during a transaction verification and will be denied. The downside to this is that it would be impossible to identify anyone who attempts to perform a double spend with fraudulent intent or as a result of software or human error. The system, however, will block such attempts.

3.1.4 Egalitarian proof of work

The CryptoNote’s proof of work mechanism is actually a voting system where users vote for the right order of transactions, new features in the protocol and honest money supply distribution. It is important that during the voting process every participant have equal voting rights.^[21] Most CryptoNote coins use the CryptoNight^[23] algorithm to run its blockchain and secure its network, the only exception being Boolberry. CryptoNight is a proof-of-work algorithm that mixes graphics processing unit (GPU) and central processing unit (CPU) mining to create a system resistant to both application-specific integrated circuits (ASICs) and fast memory-on-chip devices. This is designed to create a more uniform distribution of coins through the currency’s life. However, there are some questions about its susceptibility to botnets.

The algorithm includes:^[24]

- Keccak sponge construction;
- Script-like 2 MB scratchpad with random look-ups (read-write);
- 64-bit multiplications;
- Advanced Encryption Standard (AES) encryptions
- Hash functions BLAKE, Grøstl, JH, Skein

3.1.5 Adaptive network limits

There are no hard-coded constants in CryptoNote code. Each network limit such as maximum block size, or minimum fee amount is adjusted based on the historical data of the system. Moreover, the difficulty and the maximum block size are automatically adjusted with each new block.^[25]

3.1.6 Philosophy

CryptoNote philosophy is built on privacy as a fundamental human right, and egalitarianism.^[26] According to the *whitepaper*, the CryptoNight algorithm is intended to make the coin adhere to Satoshi Nakamoto’s original vision of “one-CPU-one-vote” system. Thus the tremendous advantage GPUs have over CPUs in most cryptocurrencies is considerably decreased in CryptoNight. If it is a good thing, or not, is debatable.^{[27][28]}

3.1.7 Current CryptoNote currencies

The CryptoNote platform has been used in several cryptocurrencies. The CryptoNote Foundation encourages developers to clone the technology. Transaction confirmation time, total number of coins and proof-of-work logic are subject to be altered in forks. Several attempts has been performed to alter core protocol: Boolberry adds address aliases and DigitalNote introduced private messaging.

Bytecoin (BCN)

Bytecoin (BCN), not to be confused Bytecoin (BTE), was the first implementation of the CryptoNote protocol launched in July 2012. Since launching, several improvements have been introduced including multisignature transactions^[29] and several security updates. In 2013, the original CryptoNote Java implementation was rewritten using C++.^[30]

The Bytecoin blockchain contains some extra information not directly related to money transfers: several blocks include geographic coordinates of universities, educational facilities among other buildings.^[31] Blocks generated since August 11, 2012 contain quotes from *Cyphernomicon*, *Neuromancer* by William Gibson and other authors.^[32]

On March 31, 2015 Bytecoin developers announced their roadmap for several upcoming releases.^[33] The following improvements were mentioned among others:-

- payment gateway capable of receiving and sending thousands transactions simultaneously
- desktop GUI wallet software (released few weeks later in April 2015^[34])
- several API layers for integration with other software
- blockchain-based aliases system
- blockchain-based assets
- smart contracts with embedded turing-complete language

Monero (XMR)

Main article: [Monero \(cryptocurrency\)](#)

Monero is currently the most well known of all the cryptonotes and has ongoing support from the community.^[35] Forked from Bytecoin in April 2014, it has a 1-minute block target and 50% slower emission speed. Monero has been praised by bitcoin core developers Gregory Maxwell, Peter Todd, and Wladimir J. van der Laan.^[36]

Along with simplewallet Monero has numerous GUI wallet applications as well as MyMonero that was launched on November 24, 2014. Monero has also teamed up with academic cryptographers,^[37] implemented an extensive aliasing system, *OpenAlias*,^[38] partially funded Privacy Solution for integrating I2P in Monero,^[39] created an anonymous voting system, URS,^[40] and implemented Electrum's mnemonic seeds.

Aeon (AEON)

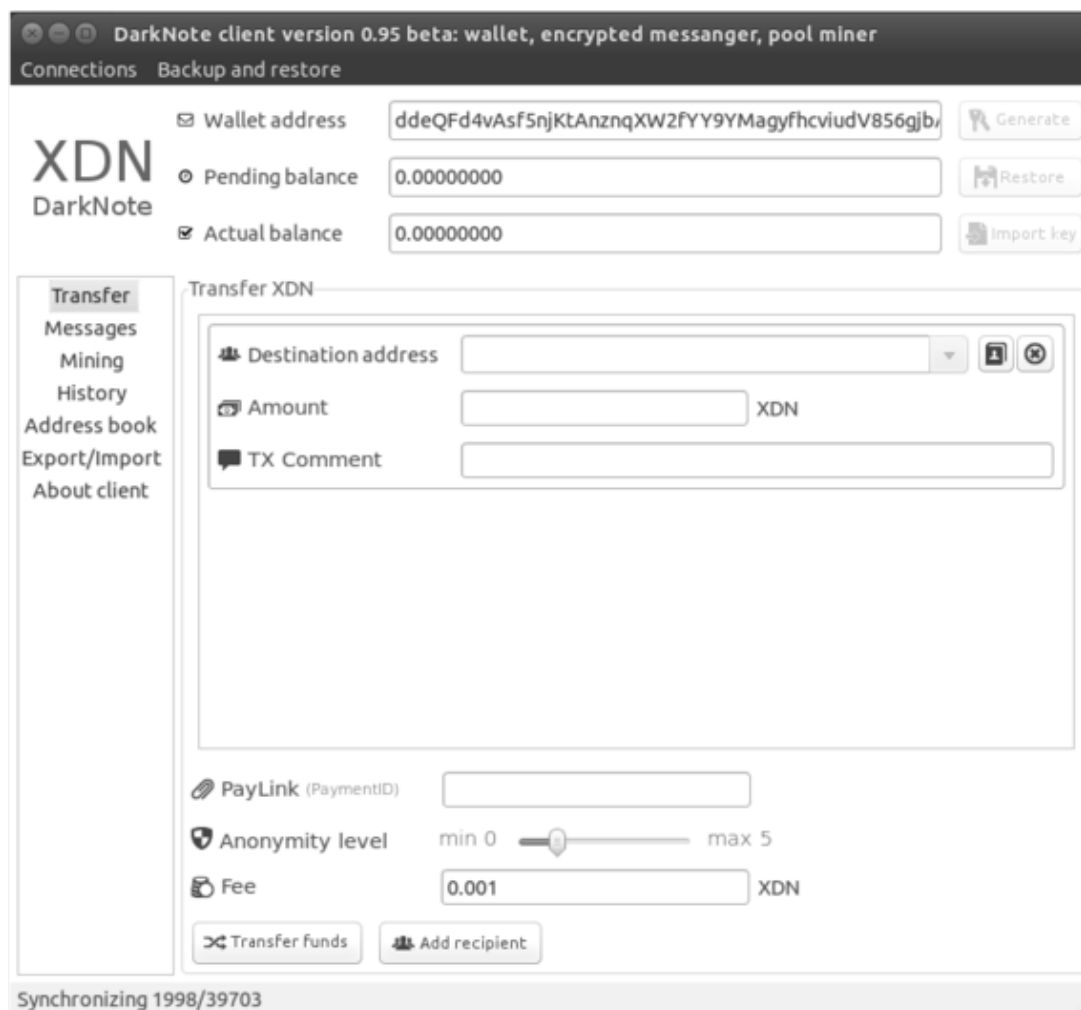
Aeon was launched on June 6, 2014 as a fork of Monero and with the same maximum supply of 18.4 million coins.^[41] It has a block time of 4 minutes and a smoothly varying reward using the formula $(M-A) / (218) / (1012)$ where $M = 264 - 1$ and $A =$ supply mined to date.^[41] Consequently, it has a similar emission curve to Monero albeit offset by about 6 weeks.^[42]

In October 2014 the original developers discontinued work on Aeon and the project was considered abandoned.^[43] However, in April 2015, after a display of community approval, all of Aeon's assets were handed over to a new core team of developers including notable developers concurrently working on the Monero project.^[44] The Aeon project was thereafter rebranded and a new roadmap announced.^[45]

Aeon has been subsequently developed with a continued emphasis on secure and scalable blockchain obfuscation in the interests of user privacy, with additional new faculties pertaining to mobile and low-fidelity operating hardware.^[45]

DigitalNote (XDN)

DigitalNote is a CryptoNote based cryptocurrency, does not follow slow block reward reduction approach of CryptoNote. It halves block reward every 11000 blocks (1 month) instead. This approach is similar to bitcoin's. About 80% of all DigitalNotes were mined in the very first year by community members and miners with the fair CPU-efficient proof-of-work. The idea is to provide main coin units amount for Crypto Economy needs in the very first year, avoiding future miners manipulation and making both network and coin units decentralized. After the first year XDN has a static block reward = 150 XDN and first blockchain banking deposits with interest rate.



DigitalNote GUI wallet

DigitalNote was launched in May 2014 as duckNote. Later duckNote was renamed to darkNote and introduced encrypted transactions comments and encrypted messaging features.^{[46][47]} Messaging functionality provided by DigitalNote is popular in regions with high social tension and total surveillance.^[48] Following the duckNote to DarkNote rebranding, the XDN price rose by about 50%.^[49] In 2015 DarkNote has been renamed again to DigitalNote.^[50]

Later a pure JavaScript paper wallet generator has been developed for DigitalNote.^[51] The resulting private key can be used with DigitalNote GUI wallet.

Also with DigitalNote XDN developers made first ever cryptocurrency blockchain *banking deposits* with interest rate on proof-of-work system.^[52]

Boolberry (BBR)

Boolberry is a Bytecoin fork with several improvements and a very intensive development. At its launch, the following improvements had been implemented:

- Wild Keccak hash function instead of CryptoNight
- user friendly address aliases are possible
- alerts from developers

DarkNetCoin (DNC)

DarkNetCoin is a fork of BoolBerry launched on October 13, 2014. It is announced as a general currency for DarkNetSpace - a platform for anonymous applications such as P2P exchange, on-chain shop, Lotto, Gamble, and Bets.^[53] DarkNetCoin inherits all features from the BoolBerry main branch: WildKeccak hash, aliases and alerts. Development roadmap includes P2P exchange, smart contracts, on-chain shops and proof-of-stake implementation. DarkNetCoin team is financed by miners: a 10% development bonus is charged from every block starting from height 4550. 1% of development bonus goes to CryptoNote team.

Quazarcoin (QCN)

Quazarcoin has been created by bitcointalk member OracionSeis as an attempt to relaunch BitMonero with a slower emission curve.^[54] 50% of Quazarcoins will be emitted during 6 years. Few months after its launch, Quazarcoin has been refocused to distributed torrent-files storage providing users with censorship-free “tracker”.

Fantomcoin (FCN)

Fantomcoin is a Bytecoin fork with merged mining support. Fantomcoin can share hashpower with any other CryptoNight-based coin. It has been released with GUI user-friendly miner and command line miner for cloud mining.

Moneta Verde (MCN)

Moneta Verde is a Bytecoin fork that implements infinite coin emission driven by its network’s hashrate and merged mining support. Moneta Verde is claimed to be environment-friendly.

Dashcoin (DSH)

A 1:1 clone of Bytecoin that claims to have “self-mutating code”. Dashcoin is automerged from Bytecoin source tree, which means that the Dashcoin codebase is always the same as Bytecoin’s. Dashcoin team released scripts generating personalized coins based on Cryptonote technology.

RedWind (RD)

RedWind is another CryptoNote Starter fork created for only one mission – funding colonization of Mars.^[55] RedWind was launched in September 2014.

Breakoutcoin (BRO)

Breakoutcoin is a fork of CryptoNote repository announced by Breakout Gaming (BRO)^[56] as a coin intended for online gaming.^[57] BreakoutCoin offers several new features in CryptoNote: Proof-of-Bergstake and BotlessNight hashing algorithm. Initial coin offering was scheduled to October 14, 2014.

CryptoNoteCoin (CNC)

CryptoNoteCoin is the official reference coin launched for educational purposes only. Official site warns users from trying to use CryptoNoteCoin for commercial purposes because coin emission restarts every 2 months.

Pebblecoin (XPB)

Pebblecoin is a CryptoNote-based coin launched in January 2015. It uses a new proof-of-work algorithm called Boulderhash that requires 13 GB RAM. Developer claims that this algorithm is protected against botnets.^[58]

Discontinued

3.1.8 Controversy and criticism

Daemon-wallet architecture

Unlike in Bitcoin, all CryptoNote currencies have functionality of network node and wallet split into two separate executables: daemon and simplewallet. Wladimir J. van der Laan writes:

“To name an example of it done right, IMO: Monero’s 'simplewallet'. It is a command-line utility wallet that communicates with the node software, and remembers where it was in the chain, and processes changes to the chain state since its last invocation when it 'refreshes'. What is nice is that one can run an arbitrary number of simplewallets against one node daemon, and unlike bitcoind’s wallet it doesn't need to run as always-on daemon itself. It can be invoked when the user wants to do something with the wallet, or see if there are new transactions.” *Bitcoin Development* (17 September 2015).

Blockchain bloat and ring signature size

The kind of ring signature used in CryptoNote grows linearly with a number of public keys used in mixing.^[64] The exact formula is $S = 64n + 32$ bytes, where n is the number of said keys (including the key of the sender). There were proposed another ring signature with a lesser size, for example Chandran signatures size is proportional to square root of n . When n is quite large, the difference becomes more significant: under particular conditions, Chandran signature is 4KB while the CryptoNote ring signature is 36KB.^[65] But as for 2015 none of the proposed algorithms are actually implemented in any cryptocurrency.

Developer of Boolberry, the CryptoNote-based coin, proposed another solution for this problem by going back and actually pruning the old signatures from the blockchain; however, said solution has not been implemented yet.[reference needed]

Nevertheless, an analogy to bitcoin’s simple payment verification is still possible: a user can avoid running full node and keeping the whole blockchain by querying the network for the Merkle branch of a transaction.

Origins

The author of the white paper went by the name Nicolas van Saberhagen, although like Satoshi Nakamoto (the author of the bitcoin white paper) that name is likely a pseudonym. Saberhagen’s true identity and location remains unknown. Some have claimed that the real creator is someone in the bitcoin community. Adam Back, Nick Szabo and even Satoshi Nakamoto^[66] himself have been floated as possible suspects,^[67] but there is little to no evidence actually supporting those claims.

Stanford Bitcoin Group’s possible involvement in creation of the CryptoNote protocol has also been discussed.^[68] Prior to CryptoNote cryptocurrency protocol, the domain **cryptonote.org** hosted an encrypted message application also named CryptoNote.^[69] This application was developed by the members of the Stanford Bitcoin Group but had not received wide recognition. This website currently hosts the CryptoNote technology.

Coin Mill conspiracy theory

Several CryptoNote-based coins launches are looking very similar: their announcement threads on bitcointalk.org forum were created by “newbie” accounts and looked alike stressing the slogans such as 'CPU-only mining' and being 'ASIC resistant'. Moreover same file sharing service used for releases. It is supposed that the only purpose of such launches was to earn easy money and creators were not intended to support and develop these forks.^[70]

Faked versions of whitepaper

Community activists discovered altered versions of CryptoNote whitepapers with digital signatures not corresponding to Nicolas van Saberhagen PGP key and missing PGP watermarks.^[71] This incident has been attributed to documents’ forgery.^[72] The possible goal of people behind this action was to refute claims about public availability of CryptoNote

since 2012 in order to gain competitive advantage.^{[71][73]} Modified whitepaper included link to discussion thread started in May, 2013 on bitcointalk.org forum and have been generated using [TeX Live](#) software released in 2013 with [XMP](#) date property set to 2014.

Bytecoin and Cicada

Bytecoin Tor site included a hidden message with a reference to Cicada 3301. Users also noticed that Cicada-style pictures were used by Bytecoin developers or by somebody impersonating them. Bytecoin blockchain contains several riddles composed of multiple messages. One of these messages possibly refers to Cicada: “And it’s the name of person you should give your key. To find it - follow little rabbit on land you've recently inhabit.”^[31]

3.1.9 See also

- [Alternative currency](#)
- [Crypto-anarchism](#)
- [Private currency](#)
- [Dark Wallet](#)
- [Zerocoin](#)

3.1.10 References

- [1] Godwin. “CryptoNote”. [Bitcoin.it](#)
- [2] “Infographics: Bytecoin and Bitcoin”.
- [3] Lee Banfield. “Research Report: The Most Ethical and Genuine Altcoins”. [Weekly Global Research](#)
- [4] Antonopoulos, Andreas (April 2014). “Chapter 9. Alternative Chains, Currencies, and Applications”. *Mastering Bitcoin. Unlocking Digital Crypto-Currencies*. ISBN 978-1-4919-0261-5.
- [5] “Bitcoin mining hardware comparison”. [bitcoin.it](#).
- [6] Nicolas van Saberhagen. “CryptoNote v 2.0” (PDF).
- [7] Nicolas van Saberhagen (2012-12-12). “CryptoNote v 1.0” (PDF).
- [8] “Programming Languages Comparison: Cryptocurrency Perspective”.
- [9] “Bytecoin development preconditions”.
- [10] Chaum, David (1983). “Blind signatures for untraceable payments” (PDF). *Advances in Cryptology Proceedings of Crypto* **82** (3): 199–203.
- [11] Ronald L. Rivest, Adi Shamir, Yael Tauman (2001-11-20). “How to Leak a Secret”.
- [12] Patrick P. Tsang, Victor K. Wei. “Short Linkable Ring Signatures for E-voting, E-cash and Attestation” (PDF). Department of Information Engineering, The Chinese University of Hong Kong
- [13] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System *” (PDF). [Bitcoin.org](#)
- [14] ByteCoin. “Untraceable transactions which can contain a secure message are inevitable”. [Bitcointalk.org](#)
- [15] Fergal Reid, Martin Harrigan. “An Analysis of Anonymity in the Bitcoin System”. [Anonymity in Bitcoin](#)
- [16] SDLerner. “Destination Address Anonymization in Bitcoin”. [Bitslog](#)
- [17] Tk Hamed (2014-04-27). “Bytecoin & Monero: Next Step to 2nd Generation Anonymity”. *Coins Source*. Retrieved 2014-10-14.
- [18] DeMartino, Ian (2014-06-24). “CryptoNote Offers More Anonymity For The Future Of Cryptocurrencies”. *CoinTelegraph*. Retrieved 2014-10-14.

- [19] Maxwell, Gregory (2013-08-22). "CoinJoin: Bitcoin privacy for the real world". *bitcointalk.org*. Retrieved 2014-10-14.
- [20] "Untraceable payments". *Cryptonote.org*
- [21] Robert Tiger (2014-08-07). "CryptoNote Currencies – Anonymous 3rd Gen". *Cryptocoinsnews.com*. Retrieved 2015-01-16.
- [22] Fujisaki, Eiichiro; Suzuki, Koutarou (2007). "Traceable Ring Signature". *Public Key Cryptography*: 181–200.
- [23] Godwin. "CryptoNight". *Bitcoin.it*
- [24] "bytecoin / src / crypto / slow-hash.c". *GitHub*.
- [25] Stanton, Andy. "Introducing CryptoNote". *cryptscout.com*.
- [26] "CryptoNote Philosophy". *cryptonote.org*.
- [27] Xulescu (2014-10-26). "Botnet argument - Xulescu".
- [28] Andrew "Andytoshi" Poelstra (2014-10-26). "ASICs and Decentralization FAQ" (PDF).
- [29] "Bytecoin (BCN) is Now Armed With Multisig".
- [30] "History of Cryptocurrency, Part I: From Bitcoin's Inception to the Crypto-Boom". *The CoinTelegraph*. 2015-04-11. Retrieved 2015-04-21.
- [31] Tk Hamed (2014-09-08). "Mysteries and Puzzles Behind the CryptoNote Technology (1/3)". *Coins Source*. Retrieved 2014-10-14.
- [32] Tk Hamed (2014-09-09). "Mining Groups in the Blockchain (Part 2 of 3)". *Coins Source*. Retrieved 2014-10-14.
- [33] Ullo (2015-03-31). "Bytecoin website and roadmap release (including CryptoNote protocol updates)". *bitcointalk.org*. Retrieved 2015-04-01.
- [34] "Bytecoin Releases GUI and Client Update". *Coins Source*. 2015-04-10. Retrieved 2015-04-21.
- [35] "Monero (XMR) CoinGecko Community Statistics". *www.coingecko.com*. Retrieved 29 September 2015.
- [36] "Wladimir J. van der Laan". *http://bitcoin-development.narkive.com/*. Retrieved 29 September 2015.
- [37] "Monero Research Labs".
- [38] "openalias".
- [39] "The-Privacy Solutions Project".
- [40] "Unique Ring Signatures using secp256k1 keys".
- [41] "[ANN] AEON 2nd gen cryptonote, anon, mobile-friendly, scalable, pruning". *bitcointalk.org*. Retrieved 2015-10-02.
- [42] "What's the current state and history of Aeon? Why should I get involved? • /r/aeoncoin". *reddit*. Retrieved 2015-10-02.
- [43] "[ANN] AEON 2nd gen cryptonote, anon, mobile-friendly, scalable, pruning". *bitcointalk.org*. Retrieved 2015-10-02.
- [44] "[ANN] AEON 2nd gen cryptonote, anon, mobile-friendly, scalable, pruning". *bitcointalk.org*. Retrieved 2015-10-02.
- [45] "[ANN] AEON 2nd gen cryptonote, anon, mobile-friendly, scalable, pruning". *bitcointalk.org*. Retrieved 2015-10-02.
- [46] "Duck goes Dark".
- [47] Tanzarian, Armand (2014-09-22). "Altcoins We Are Excited About: An Introduction to DarkNote". *CoinTelegraph*. Retrieved 2014-10-14.
- [48] Cuthbertson, Anthony (2015-07-16). "Dissidents turn to bitcoin-like cryptocurrency to communicate free from state surveillance". *International Business Times (IBTimes)*. Retrieved 2015-08-05.
- [49] Wilmoth, Josiah (2014-09-21). "DuckNote Price Launches After DarkNote Reinvention". *CryptoCoinsNews*. Retrieved 2014-10-14.
- [50] "Darknote rebranding". 2015-07-17.
- [51] "DarkNote paper wallet generator announcement". 2014-12-17.

- [52] DeFranco, Michael (2015-08-26). "Messaging And Mobile In Financial Services". *Forbes.com*. Retrieved 2015-09-01.
- [53] "[ANN][DNC][GPU/CPU]DarkNetCoin-NOPREMINED-NO IPO-True anonymity". 2014-10-10.
- [54] "[QCN] Quazarcoin".
- [55] "[ANN][RD] RedWind / Colonization of Mars."
- [56] Lopez, Jaime (2014-10-14). "A New Virtual Currency Launched from Costa Rica". *The Costa Rica Star* (San José, Costa Rica).
- [57] "[ANN][BRO] *ICO* Breakout". *bitcointalk.org*.
- [58] "Pebblecoin (XPB) - Botnet Resistant - Cryptonote, Wallet GUI!". *bitcointalk.org*.
- [59] "[ANN] [DB] Doctor Who ? DoctorByte ! VISIT DOCTORBYTE.CO NOW".
- [60] "[INF8] Infinium-8. Privacy-centric & CPU-mining". *bitcointalk.org*.
- [61] Cordell, Drew (2014-08-09). "CryptoNoteCoin; CryptoNote Technology From Within". *The Cryptocoin Chronicle*.
- [62] "[MNT] MountCoin - [ANONYMOUS - CRYPTONIGHT - NO IPO/PREMIENE]".
- [63] "OneEvilCoin OEC Information".
- [64] "Can Anoncoin Be The Currency Of The Deep Web?".
- [65] "StealthCoin Unique Kind Take On Crypto-Currency Anonymity".
- [66] "Bytecoin: Satoshi's New Project". *thebitcoinnews.com*. 2014-11-24. Archived from the original on 2014-12-05. Retrieved 2015-03-24.
- [67] "Bytecoin Source of origin". *bytecoiner.org*. Retrieved 2014-10-14.
- [68] Ackerman, Ronald. "Stanford Wide Gate Steep Steps".
- [69] "CryptoNote - Send and receive single-view, encrypted messages". Archived from the original on 2013-10-20.
- [70] "How to invest in altcoins without losing everything".
- [71] "Negative PR Techniques At Work: An Attack on CryptoNote". 2014-09-28.
- [72] "Statement from the CryptoNote team". 2014-08-21.
- [73] "Cryptocurrency 2.0 Basics: Protocols and Platforms Inspired by Bitcoin". 2014-06-17.

3.2 Monero (cryptocurrency)

Monero (XMR) is a cryptocurrency created in April 2014 that is focused on privacy, decentralisation and scalability. Unlike many cryptocurrencies that are derivatives of Bitcoin, Monero is based on the CryptoNote protocol and possesses significant algorithmic differences relating to blockchain obfuscation.^[4] Monero has ongoing support from the community,^[5] and its modular code architecture has been praised by Wladimir J. van der Laan, the Bitcoin Core maintainer.^[6] Monero currently carries a market capitalization of over \$4 million.^[7]

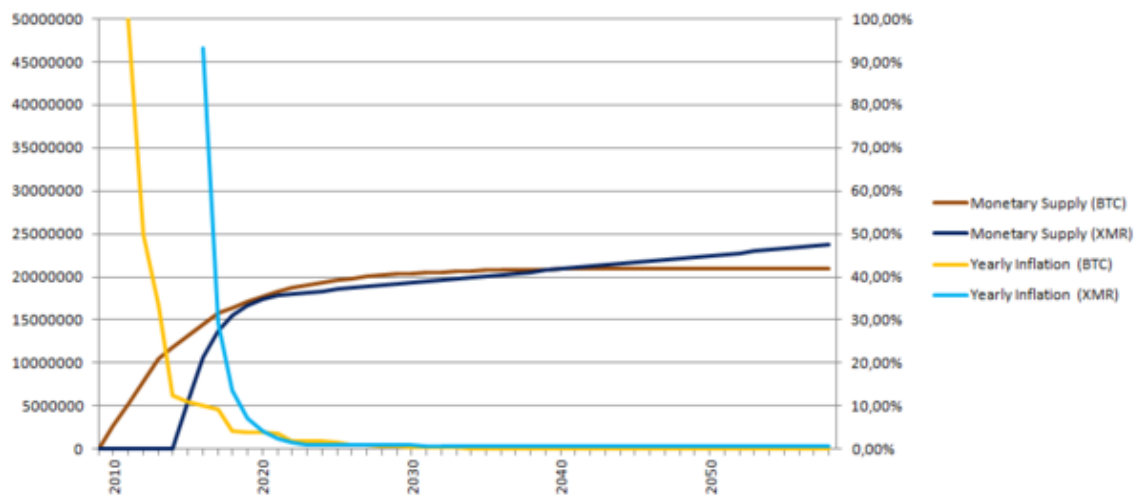
3.2.1 History

Monero was launched on 18 April 2014^[8] originally under the name **BitMonero**, which is a compound of Bit (as in Bitcoin) and Monero (literally meaning coin in Esperanto). Five days later the community opted for the name to be shortened just to **Monero**.^{[9][10]} It was launched as the first fork of CryptoNote-based currency Bytecoin, however was released with two major differences. Firstly, the target block time was decreased from 120 to 60 seconds, and secondly, the emission speed was decelerated by 50%. In addition, the Monero developers found numerous incidents of poor quality code that was subsequently cleaned and re-constituted.

A few weeks after launch, an optimized GPU miner for CryptoNight proof-of-work function was developed.^[11]

On 4 September 2014, Monero recovered from an unusual and novel attack^[12] executed against the cryptocurrency network.^[13]

3.2.2 Features



Monero coin supply and inflation over time.

Monero is an open-source pure proof-of-work cryptocurrency. It runs on Windows, Mac, Linux and FreeBSD.^[14]

Its main emission curve will issue about 18.4 million coins to be mined in approximately 8 years.^[15] After that, a “tail emission” will create a sub-1% perpetual inflation to prevent the lack of incentives for miners once a currency is not mineable anymore.^[16] The emission uses a smoothly decreasing reward with no block halving (any block generates a bit less moneroj than the previous one). The proof-of-work algorithm, **CryptoNight**, is AES-intensive and “memory heavy”, which significantly reduces the advantage of GPU over CPU.

Privacy



The changes in the results of blockchain analysis after implementing the ring signatures.

Monero daemon uses the original **CryptoNote** protocol except for the initial changes (as the block time and emission speed). The protocol itself is based on “one-time ring signatures”^[17] and stealth addresses. Underlying cryptography is essentially Daniel J. Bernstein's library for Ed25519, which is Schnorr signatures on the Twisted Edwards curve. The end result is passive, decentralised mixing based on heavily-tested algorithms.^[18]

However, several improvements were suggested by Monero Research Labs (a group of people, including core developers team), which covered the proper use of ring signatures for better privacy.^[19] Specifically, the proposals include “a protocol-level network-wide minimum mix-in policy of $n = 2$ foreign outputs per ring signature”, “a nonuniform transaction output selection method for ring generation” and “a torrent-style method of sending Monero output”.^[20] If implemented, these changes, as stated by the authors, can help protect user's privacy in a CryptoNote-based currency.

As a consequence, Monero features an opaque blockchain (with an explicit allowance system called the *viewkey*), in sharp contrast with transparent blockchain used by any other cryptocurrency not based on **CryptoNote**. Thus, Monero is said to be “private, optionally transparent”. On top of very strong privacy by default, such a system permits **net neutrality** on the blockchain (miners cannot become censors, since they do not know where the transaction goes or what it contains) while still permitting auditing when desired (for instance, tax audit or public display of the finances of an NGO).^[21]

Monero developers are also working on implementing a C++ **i2p** router straight in the code. This would complete the privacy chain by also hiding the IP addresses.^[22]

Decentralisation

The smart mining^[23] forthcoming feature will allow transparent CPU mining on the user’s computer, far from the de facto centralization of mining farms and pool mining, pursuing Satoshi Nakamoto’s original vision of a true p2p currency.^[24]

Scalability

Monero has no hardcoded limit, which means it doesn't have a 1 MB block size limitation preventing scalability.

The Monero Core Team also released a standard called **OpenAlias**,^[25] which permits much more human-readable addresses and “squares” the **Zooko’s triangle**. **OpenAlias** can be used for any cryptocurrency and is already implemented in Monero, Bitcoin (in latest Electrum versions) and **HyperStake**, as well as several websites such as mymonero.com and coin.space.

3.2.3 Usage

XMR.TO allows you to make a payment to any Bitcoin address with the strong privacy provided by Monero.^[26]

3.2.4 Limitations

Since it is not based on Bitcoin, Monero cannot take advantage of the Bitcoin technological ecosystem, like GUI wallet or payment processors. As a consequence, everything has to be written from scratch.^[27] Presently (as of March 2015), Monero doesn't have feature parity with Bitcoin. Notably, there is no support to multisignature and no Monero payment processor (but in April 2015 it was announced on bitcointalk.org one is in the works by a member of The Monero Core Team^[28]).

3.2.5 Ongoing work and side projects

- MoneroX: a .Net based GUI wallet software offers sending/receiving coins functionality. MoneroX uses RPC connection to network nodes and provides interface that looks like traditional Bitcoin-Qt client;^[29]
- OpenAlias: an extensive aliasing blockchain-based system;^[30]
- Partially funded Privacy Solution for integrating I2P in Monero;^[31]
- URS: the proof-of-concept of an anonymous voting system, based on ring signatures;^[32]
- Electrum’s mnemonic seeds for deterministic key creation in webwallet;^[33]
- The Monero Core Team continues to depart from the original Bytecoin code with numerous patches and improvements to its implementation of the **Cryptonote** protocol.^{[34][35]}

3.2.6 Applications

CryptoKingdom is a MMORPG that uses Monero for entry into its economy.^[36]

MoneroDice is a dice gambling game that uses cryptography for provably fair randomness.^[37]

3.2.7 See also

- Alternative currency
- Alternative Finance
- Anonymous Internet banking
- Crypto-anarchism
- Decentralized autonomous organization
- Electronic money
- Private currency
- Proof-of-work system
- World currency

3.2.8 External links

- Official website for Monero

3.2.9 References

- [1] "An Investor's Investigation Into The Mining Statistics Of Bitcoin Alternatives - Monero" Check `lurl=` value (help). *dev-tome.com*. Retrieved 2 April 2015.
- [2] "Monero Announcements Thread". *bitcointalk.org.com*. Retrieved 8 November 2015.
- [3] Latapie, David. "Submultiples of Monero". *getmonero.org*. Retrieved 3 April 2015.
- [4] "Nope. You are confused. You should consider this great news because you are abou... | Hacker News". *news.ycombinator.com*. Retrieved 2015-10-04.
- [5] "Monero (XMR) CoinGecko Community Statistics". *www.coingecko.com*. Retrieved 29 September 2015.
- [6] "Wladimir J. van der Laan". *http://bitcoin-development.narkive.com/*. Retrieved 29 September 2015.
- [7] "Monero (XMR) Market Capitalization". *www.coinmarketcap.com*. Retrieved 29 September 2015.
- [8] "[ANN][BMR] Bitmonero - a new coin based on CryptoNote technology - LAUNCHED". *bitcointalk.org*. Retrieved 10 May 2014.
- [9] Latapie, David. "[ANN][BMR] Bitmonero - a new coin based on CryptoNote technology - LAUNCHED". *bitcointalk.org*. Retrieved 1 April 2015.
- [10] "[ANN][MRO] Monero - Anonymous Currency Based on Ring Signatures". *bitcointalk.org*. Retrieved 20 May 2014.
- [11] Andersen, David. "Minting Money with Monero ... and CPU vector intrinsics". *da-data.blogspot.ru*. Retrieved 30 March 2015.
- [12] "[XMR] Monero - A secure, private, untraceable cryptocurrency (mandatory upgrade)". *bitcointalk.org*. Retrieved 4 April 2015.
- [13] Macheta, Jan; Noether, Surae; Noether, Sarang; Smooth, Javier. "Counterfeiting via Merkle Tree Exploits within Virtual Currencies Employing the CryptoNote Protocol" (PDF). *getmonero.org*. Retrieved 4 April 2015.
- [14] Latapie, David. "What's so special about Monero". *Getmonero.org*. Retrieved 19 March 2015.
- [15] "Monero Economy". *bitcointalk.org*. Retrieved 4 April 2015.
- [16] Hutchinson, Martin. "Breakingviews: Bitcoin's defects will hasten its demise in 2015". *reuters.com*. Retrieved 19 March 2015.
- [17] Saberhagen, Nicolas. "CryptoNote" (PDF). *cryptonote.org*. Retrieved 5 October 2015.

- [18] Spagni, Riccardo. "Alright devs, own up: what's the deal with "magic" block 202612?". *Reddit*. Retrieved 29 March 2015. Based on our current level of technology and our current understanding of cryptography there is no vulnerability in ring signatures, not in theory nor in our implementation (which is mostly based on old, exceedingly well-tested cryptography and code from SUPERCOP / libsodium / NaCL). The cryptography is directly based on work that is nearly 10 years old, which in turn is grounded in cryptography in a paper from 1991, so we're talking about something that has already been analysed by very gifted cryptographers.
- [19] "Monero Research Labs". *getmonero.org*. Monero. Retrieved 31 March 2015.
- [20] Mackenzie, Adam; Noether, Surae; Monero Core Team. "Improving Obfuscation in the CryptoNote Protocol" (PDF). *getmonero.org*. Retrieved 31 March 2015.
- [21] Latapie, David. "March FinTech Open Mic Night - Monero". *youtube.com*. Retrieved 4 April 2015.
- [22] Latapie, David. "Why we chose i2p over TOR". *getmonero.org*. Retrieved 19 March 2015.
- [23] "[ANN][MRO] Monero - Anonymous Currency Based on Ring Signatures". Retrieved 5 April 2015.
- [24] "Bitcoin whitepaper". Retrieved 5 April 2015.
- [25] "OpenAlias official website". *openalias.org*. Retrieved 19 March 2015.
- [26] "What is XMR.TO?". *xmr.to*. Retrieved 5 April 2015.
- [27] Latapie, David. "Why is the official GUI wallet not released yet". *getmonero.org*. Retrieved 19 March 2015.
- [28] Spagni, Riccardo. "[XMR] Monero - A secure, private, untraceable cryptocurrency - 0.8.8.6". *bitcointalk.org*. Retrieved 3 April 2015.
- [29] "[XMR] MoneroX - A cross platform graphical account manager for Monero".
- [30] "OpenAlias official website". *getmonero.org*. Retrieved 30 March 2015.
- [31] "The-Privacy Solutions Project". *geti2p.net*. Retrieved 30 March 2015.
- [32] "Unique Ring Signatures using secp256k1 keys". *bitcointalk.org*. Retrieved 30 March 2015.
- [33] "MyMonero". *mymonero.com*. Retrieved 30 March 2015.
- [34] Spagni, Riccardo. "[XMR] Monero - A secure, private, untraceable cryptocurrency - 0.8.8.6". *bitcointalk.org*. Retrieved 4 April 2015.
- [35] "Github - monero-project". *github.com*. Retrieved 4 April 2015.
- [36] <https://cryptokingdom.me>
- [37] <https://monerodice.net/>

Chapter 4

Other proof-of-work

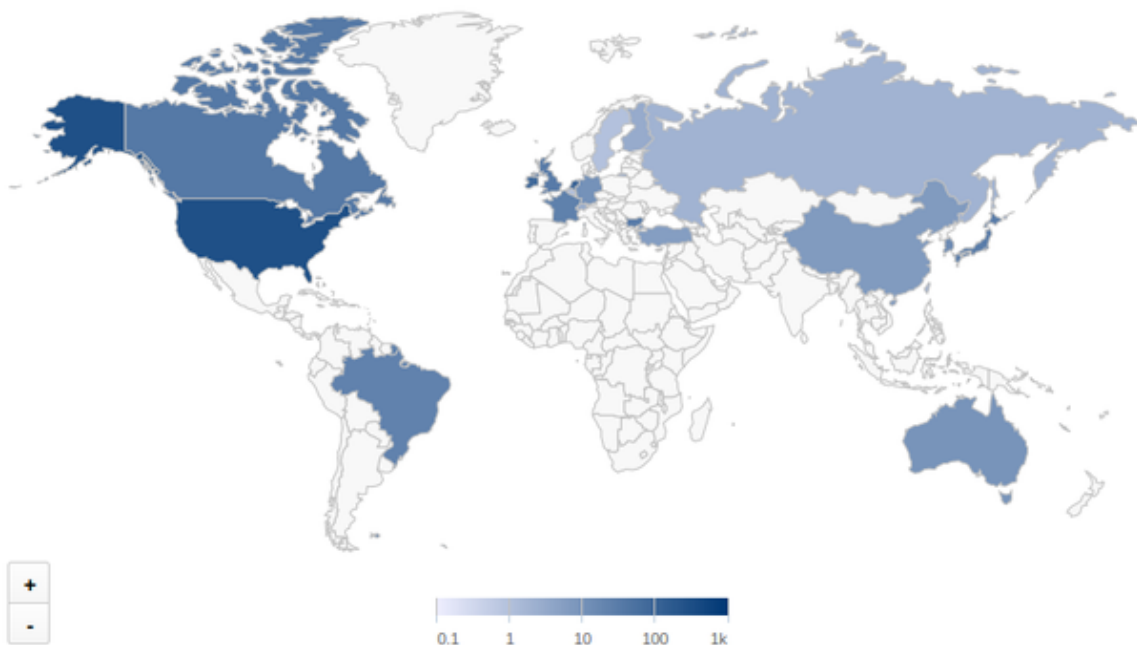
4.1 Dash (cryptocurrency)

Dash (formerly known as **Darkcoin** and **XCoin**) is an open source peer-to-peer cryptocurrency that uses a system called Darksend to add privacy to transactions.^[1] It was rebranded from “Darkcoin” to “Dash” on March 25, 2015, a portmanteau of “Digital Cash”.^[2]

Dash uses a chained hashing algorithm approach called X11 for the proof-of-work. Instead of using the SHA-256 (from well-known Secure Hash Algorithm family) or scrypt it uses 11 rounds of different hashing functions.^[3]

4.1.1 Overview

Darksend



Masternode count by country (as of September 2014)

Darksend is a coin-mixing service originally based on CoinJoin. Later iterations used a more advanced method of pre-mixing denominations built into the user’s wallet.

In its current implementation it adds privacy to transactions by combining identical inputs from multiple users into a single transaction with several outputs. Due to the identical inputs, transactions usually cannot be directly traced,

obfuscating the flow of funds. A heuristic (based on inputs/outputs order) was suggested for partial tracing the transactions, but neither formal proof nor counter-proof was presented.^[4]

Masternodes

Darksend's mixing is performed by Masternodes, servers operating on a decentralized volunteer network which have the responsibility of signing the transactions. For each round of Darksend, the user selects two to eight (or even more) rounds of mixing which vary the degree of anonymity achieved. Random Masternodes are then elected to perform the coin mixing. Masternodes are trust-less, in the sense that they cannot steal user coins, and the combination of multiple Masternodes ensures that no single node has full knowledge of both inputs and outputs in the transaction process.

To avoid a "bad actor" scenario, in which many Masternodes are operated by an adversary who wants to de-anonymize transactions, a deterrent has been put in place in which 1000 Dash are required to own and operate a Masternode.^[5] As an incentive for operating a Masternode, chosen nodes currently earn 50% of the mining rewards.^[6]

InstantX

InstantX is a service that allows for near-instant transactions. Through this system, inputs can be locked to only specific transactions and verified by consensus of the Masternode network. Conflicting transactions and blocks are rejected. If a consensus cannot be reached, validation of the transaction occurs through standard block confirmation. InstantX purportedly solves the double-spending problem without the longer confirmation times of other cryptocurrencies such as Bitcoin.^[7]

X11

X11 is a hashing algorithm created by Dash core developer Evan Duffield. X11's chained hashing algorithm approach utilizes a sequence of eleven cryptographic hashing algorithms for the proof-of-work. This is so that the processing distribution is fair and coins will be distributed in much the same way Bitcoin's were originally.

With chained hashing, high end CPUs give an average return similar to that of GPUs. Another side effect of the algorithm is that GPUs run at about 30% less electrical power than script and 30% to 50% cooler, putting less stress on the computing setup and ensuring lower energy bills for miners.^[8]

Dark Gravity Wave (DGW)

Dark Gravity Wave (DGW) is a mining difficulty adjustment algorithm created by Dash core developer Evan Duffield to address flaws in Kimoto's Gravity Well. It uses multiple exponential moving averages and a simple moving average to smoothly adjust the difficulty, which is re-targeted every block. The block reward is not adjusted strictly by block number, but instead uses a formula controlled by Moore's law: $2222222/((\text{Difficulty}+2600)/9)^2$.^{[9][10]}

4.1.2 History

Dash was originally released as XCoin (XCO) on January 18, 2014. On February 28, the name was changed to "Darkcoin". On March 25, 2015, Darkcoin was rebranded as "Dash".^[2]

I discovered Bitcoin in mid 2010 and was obsessed ever since. After a couple of years in 2012 I started really thinking about how to add anonymity to Bitcoin. I came up with maybe 10 ways of doing this, but I soon realized that Bitcoin would never add my code. The developers really want the core protocol to stay the same for the most part and everything else to be implemented on the top of it. This was the birth of the concept of Darkcoin. I implemented X11 in a weekend and found it worked pretty well and it would give a completely fair start to the currency. What I really was aiming for with X11 is a similar development curve where miners would fight to create small advantages much like the early start of Bitcoin. I think this a requirement to create a healthy ecosystem.

Evan Duffield, March 2014 ^[11]

Launch

Within the first hour of launch, approximately 500,000 coins were mined, followed by another 1,000,000 coins in the next 7 hours and finally another 400,000 in 36 hours. All told 1.9 million coins were mined in 48 hours, or approximately 32% of a current supply (as of October 2015) of approximately 5.9 million,^{[12][13]} generating controversy regarding the initial distribution of coins. In June 2014, industry news site *Cryptocoinsnews* wrote “One of the biggest bumps in the road Darkcoin faces is their big instamine.”^[14] According to Duffield, this was the result of an error in the code “which incorrectly converted the difficulty, then tried using a corrupt value to calculate the subsidy, causing the instamine”.^[15]

4.1.3 References

- [1] Greenberg, Andy. Bitcoin’s nefarious cousin Darkcoin is booming *Wired*, San Francisco. 22 May 2014
- [2] “Darkcoin Is Now Dash | Dash – Official Website”. *www.dashpay.io*. Retrieved 3 April 2015.
- [3] Bentley, Guy. Darkcoin: The cryptocurrency putting privacy first, *City AM*, London. 12 May 2014
- [4] Evil-Knievel. “[DRK] Darkcoin is NOT Anonymous? Possible Proof inside”. *bitcointalk.org*. Retrieved 23 April 2015.
- [5] “DarkSend”. Dash Ninja Wiki. Retrieved 22 April 2015.
- [6] “DASH Ninja - Blocks Masternodes Payee”. DASH Ninja. Retrieved 24 September 2015.
- [7] InstantX - Transaction Locking and Masternode Consensus: A Mechanism for Mitigating Double Spending Attacks *dashpay.io*
- [8] Duffield, Evan; Diaz, Daniel (20 April 2015). “Dash: A Privacy-Centric Crypto-Currency” (PDF). Self-published.
- [9] “Dark Gravity Wave - Dash – Official Website”. *Dash - Official Website*.
- [10] How Is Darkcoin Mining Unique? *coinbrief.net*. Retrieved 30 December 2014.
- [11] Duffield, Evan. “The birth of Darkcoin”. *https://dashtalk.org*. External link in |website= (help)
- [12] “Dash Blockchain Explorer - Inflation Chart”. *cryptoID.info*.
- [13] <http://dashdot.io/alpha/wp-content/uploads/2015/05/image18.png>
- [14] “Litecoin vs. Darkcoin: Can the Coins Compete?”. *CCN: Financial Bitcoin & Cryptocurrency News*. 24 June 2014.
- [15] “Was The Instamine A Positive Thing For Dash?”. *dashdot.io*. 27 September 2015.

4.1.4 External links

- Official website

4.2 Primecoin

Primecoin (sign: **Ψ**; code: **XPM**) is a peer-to-peer open source cryptocurrency that implements a unique scientific computing proof-of-work system.^[2] Primecoin’s proof-of-work system searches for chains of prime numbers.^[2] Primecoin was created by a person or group of people who use the pseudonym Sunny King. This entity is also related with the cryptocurrency Peercoin.^{[3][4]} The Primecoin source code is copyrighted by a person or group called “Primecoin Developers”, and distributed under a conditional MIT/X11 software license.^[5]

Primecoin has been described as the main cause of spot shortages of dedicated servers because at the time it was only possible to mine the currency with CPUs.^{[1][6]} For the same reason, Primecoin used to be the target of malware writers.^{[7][8]}

On March 29, 2014 the first GPU miner^[9] became publicly available.^[10] Currently there are many GPU miners available both in solo and pool mining variations.

4.2.1 Features

When comparing Primecoin with today's most widely spread cryptocurrency called bitcoin some notable differences are:

Scarcity is governed by the nature of prime number distribution

Almost all cryptocurrencies in existence define their scarcity properties merely by set of predefined values in source code, whereas scarcity of Primecoin is based purely on a relationship of a simple function and mathematical property of natural occurrence of prime chains in the set of whole numbers that are.

No predefined ultimate number of coins Instead of having hard-set ultimate number of coins in its code like many other alternative cryptocurrencies, number of Primecoins released per block is always equal to 999 divided by the square of the difficulty.^[11] There has been some attempts at approximating this number. The number of Primecoins that will be mined will be determined by the progress of its adaptation by the mining community, improvements that will be done to the mining algorithms and ultimately by Moore's law.

Difficulty adjustment is more frequent Primecoin protocol adjusts its difficulty slightly after every block. The difficulty change that occurs each block is targeted at achieving target of one new block created once per minute.^[11] As comparison the bitcoin protocol adjusts its difficulty every 2016 blocks, or approximately every two weeks.

Faster transaction confirmations Since Primecoin blocks are generated 8 to 10 times as fast as bitcoin blocks on average, Primecoin transactions are confirmed approximately 8 to 10 times as fast.^[11]

4.2.2 Proof-of-work system

Primecoin uses the finding of prime chains composed of Cunningham chains and bi-twin chains for proof-of-work, which can lead to useful byproducts.^{[2][11]}

The system is designed so that the work is efficiently verifiable by all nodes on the Primecoin network.^[2] To meet this requirement, the size of the prime numbers in the system cannot be too large.^[2] The Primecoin proof-of-work system has the following characteristics:

- Primecoin's work takes the form of prime number chains.^[11]
- Finding the prime number chains becomes exponentially harder as the chain length is increased.^[2]
- Verification of the reasonably sized prime number chains can be performed efficiently by all network nodes.^[2]
- Mersenne primes are precluded due to their extremely large size.^[2]
- Three types of prime number chains are accepted as proof-of-work:^[11]
 1. Cunningham chain of the first kind.
 2. Cunningham chain of the second kind.
 3. Bi-twin chain.

Other cryptocurrencies including bitcoin commonly use a Hashcash type of proof-of-work based on SHA-256 hash calculations, which are of no value beyond its own economy.^{[2][11]}

List of largest known Cunningham chains of given length^[12] includes several results generated by Primecoin miners.^[13]

4.2.3 See also

- Anarcho-capitalism
- Anonymous Internet banking
- Alternative currency

- Crypto-anarchism
- Money supply
- Moore's law
- Prime number
- Cunningham chain

4.2.4 References

- [1] Clark, Jack (2013-07-16). "Virtual currency speculators shut down cloud". *The Register*. Retrieved 2014-02-02.
- [2] King, Sunny (pseudonym) (2013-07-07). "Primecoin: Cryptocurrency with Prime Number Proof-of-Work" (PDF). Retrieved 2013-11-07.
- [3] Bradbury, Danny (2013-01-02). "Why are so many digital currency players anonymous?". *CoinDesk*. Retrieved 2014-03-14.
- [4] Gilson, David (2013-07-10). "New currency Primecoin searches for prime numbers as proof of work". *CoinDesk*. Retrieved 2014-02-08.
- [5] Primecoin Developers (2013-07-25). "Primecoin High Performance 0.1.1 BETA README" (Text file). *Primecoin High Performance – Browse /0.1.1-hp8 at SourceForge.net* (mikaelh2). Retrieved 2014-02-11.
- [6] Miller, Rich (2013-12-17). "Currency Miners Cause Spot Shortages of Dedicated Servers". *Data Center Knowledge*. Retrieved 2013-12-18.
- [7] Muncaster, Phil (2014-01-17). "Bitcoin's so over. We're mining Primeco... Oh SNAP, my box is a ZOMBIE!". *The Register*. Retrieved 2014-02-02.
- [8] Goodin, Dan (2013-12-17). "What a successful exploit of a Linux server looks like". *Ars Technica* (Condé Nast). Retrieved 2014-02-02.
- [9] "primegpu.com". *www.primegpu.com*. Retrieved 2015-09-25.
- [10] "Primecoin GPU miner: 9.1 CPD on a 280x / pool / 2% dev.fee". *bitcointalk.org*. Retrieved 2015-09-25.
- [11] Buterin, Vitalik (2013-07-08). "Primecoin: the cryptocurrency whose mining is actually useful". *Bitcoin Magazine* (Coin Publishing Ltd.).
- [12] Augustin, Dirk. "Cunningham Chain records". *primerecords.dk*.
- [13] "Record Primes". *primecoin.io*.

4.2.5 External links

- Official website
- Official Primecoin white paper

4.3 Ethereum

Ethereum is a cryptocurrency which includes a programmable smart contract platform.^[1] The unit of currency is called the **ether**.

Ethereum was initially described by Vitalik Buterin in late 2013,^[2] formally described by Gavin Wood in early 2014 in the so-called "yellow paper"^[3] and launched 30 July 2015.^[4] It is among a group of "next generation" (or "Bitcoin 2.0") platforms.^[5]

4.3.1 Purpose

The intended purpose of the Ethereum Project is to build and proliferate a decentralised and pseudonymous replacement for the **World Wide Web**: incentivized static content publication (Swarm), pseudonymous low-level messaging system (Whisper), trustless transactions (Ethereum) and an integrated user-interface (Mist).^[6]

4.3.2 Development



Group photo from DEVCON-0, Berlin, 14 November 2014.

Ethereum is an open source project. Development began in December 2013, with the first Go and C++ proof of concept builds (PoC1) being released in early February 2014.^[7] Since then, several further PoC builds have been released, culminating with the public launch of the Ethereum blockchain on 30 July 2015.

4.3.3 Ether

The currency unit of Ethereum is the *ether*, used to pay for computational services on the network.

To finance development, Ethereum distributed the initial allocation of ether via a 42-day public crowdsale, netting 31,591 bitcoins, worth \$18,439,086 at that time, in exchange for about 60,102,216 ether.^[12]

4.3.4 Contracts

Smart contracts are programs and protocols to facilitate the automated performance of a contract. Ethereum contracts can be implemented in various languages, compiled into bytecode for the Ethereum Virtual Machine before being deployed to the blockchain.

Every contract is run on every full Ethereum node simultaneously and the result is the consensus of the output. The documentation notes that computation on the EVM is “very expensive” and that “you will not be able to do anything on the EVM that you cannot do on a smartphone from 1999.”^[13]

4.3.5 Implementations

The following full-node implementations of Ethereum are available:

- Geth, written in Go^[14]
- Eth, written in C++^[15]
- Ethereum J, written in Java^[16]
- pyethapp, written in Python^[17]
- ethereumjs, written in JavaScript^[18]
- ethereumH, written in Haskell^[19]

4.3.6 Media

The platform has been covered in The Wall Street Journal,^[20] *Wired*,^[21] *The Globe and Mail*,^[22] SiliconANGLE,^[23] Al Jazeera,^[24] *The Telegraph*^[25] and the *Keiser Report*.^[26]

4.3.7 References

- [1] Buterin, Vitalik. “The Problem of Censorship”. Ethereum Blog. Retrieved 6 June 2015.
- [2] Buterin, Vitalik (2014-01-23). “Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform”. *Bitcoin Magazine*. Retrieved 9 April 2014.
- [3] Wood, Gavin (2014-04-06). “Ethereum: A Secure Decentralised Generalised Transaction Ledger” (PDF). *Self published*. Retrieved 20 February 2015.
- [4] Tual, Stephan. “Ethereum Launches”. *blog.ethereum.org*. Retrieved 31 July 2015.
- [5] Kharif, Olga (2014-03-28). “Bitcoin 2.0 Shows Technology Evolving Beyond Use as Money”. *Bloomberg News*. Retrieved 11 April 2014.
- [6] Gerring, Taylor (2014-08-18). “building the decentralized web 3.0”. Retrieved 20 April 2015.
- [7] Tual, Stephan. “C++ Code+Build FAQ”. Ethereum. Retrieved 3 September 2014.
- [8] What is ether?
- [9] Genesis block
- [10] The Issuance Model in Ethereum
- [11] “The symbol for Ether is...”. 7 June 2014. Retrieved August 14, 2014.
- [12] “Crypto 2.0 Roundup: Block Chain Bloat, Ethereum Completes Presale and a Crypto Football Team”. *CoinDesk*. Retrieved 2015-11-13.
- [13] <https://github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial>
- [14] go-ethereum homepage
- [15] Ethereum C++ Client GitHub repository
- [16] Ethereum J homepage
- [17] pyethapp GitHub repository
- [18] ethereumjs homepage
- [19] ethereum-client-haskell GitHub repository
- [20] Paul Vigna (28th October 2015). Microsoft to Offer Ethereum Based Services. The Wall Street Journal. Retrieved 7 November 2015.

- [21] Finley, Kurt (2014-01-27). “Out in the Open: Teenage Hacker Transforms Web Into One Giant Bitcoin Network”. *Wired*. Retrieved 6 April 2014.
- [22] Gray, Jeff (2014-04-07). “Bitcoin believers: Why digital currency backers are keeping the faith”. *The Globe and Mail* (Phillip Crawley). Retrieved 6 April 2014.
- [23] Cox, Ryan. “Can Ethereum kill Bitcoin with self-executing contracts?”. *SiliconANGLE*. Retrieved 6 April 2014.
- [24] Nathan Schneider (7 April 2014). Code your own utopia: Meet Ethereum, bitcoin’s most ambitious successor. Al Jazeera America. Retrieved 10 June 2014.
- [25] Soon, the internet will be impossible to control. Jamie Bartlett. Retrieved 19 December 2014.
- [26] Keiser Report: New Crypto Phenomenon Ethereum. Max Keiser. Retrieved 10 June 2014.

4.3.8 External links

- Official website

Chapter 5

Non proof-of-work

5.1 BlackCoin

BlackCoin is a peer-to-peer cryptocurrency. BlackCoin uses a proof-of-stake system and is open-source.^[3] BlackCoin was created by the developer Rat4, with the goal of proving that BlackCoin's way of disabling proof-of-work is stable and secure.^[4] BlackCoin secures its network through a process called "minting". Transactions in BlackCoin were called "significant" in a Citibank whitepaper.^[5]

5.1.1 Proof-of-Stake

The expected time for a confirmation is 64 seconds while Bitcoin's expected confirmation time is 10 minutes.^[6] BlackCoin's Proof of Stake system secures the protocol through an efficient, decentralized process called "minting," while Bitcoin uses a mining process that has been well documented as expensive and energy-intensive.^{[7][8]}

5.1.2 Merchant adoption

In June 2014, BlackCoin was accepted onto Coinkite exchange and payment hardware terminals. The Coinkite terminal looks like the familiar handset device used in point of sale transactions. Coinkite's system uses these ordinary merchant terminals to accept Coinkite debit cards loaded with Bitcoin, Litecoin and BlackCoin.^[9]

5.1.3 See also

- Alternative currency
- Peer-to-peer computing

5.1.4 References

- [1] Vasin, Pavel (2014-02-16). "[ANN] BlackCoin (BC) | PoS | No premine | No IPO". *bitcointalk.org*.
- [2] "BitBeat: Blackcoin Tries to Stake Its Proof as Legit Bitcoin Alternative". *blogs.wsj.com*. 2014-07-24.
- [3] "Bitcoin Is Put Under the Microscope by Its Supporters". *PaymentsSource.com*. 2014-07-22.
- [4] "Interview with the Creator of Blackcoin". *Followthecoin.com*. 2014-07-24.
- [5] "Citi GPS: Global Perspectives & Solutions. Druptive Innovations II: Ten More Things to Stop and Think About". *ir.citi.com*. 2014-07-24.
- [6] "Bitcoin Is Put Under the Microscope by Its Supporters". *PaymentsSource.com*. 2014-07-22.
- [7] "BitBeat: Blackcoin Tries to Stake Its Proof as Legit Bitcoin Alternative". *blogs.wsj.com*. 2014-07-24.

[8] “UK Telegraph: LXC Coin crowdfunds in challenge to Bitcoin”. *www.telegraph.co.uk*. 2014-09-16.

[9] “A Popularity Content Drives Coinkite’s Digital Currency Decisions”. *PaymentsSource.com*. 2014-07-24.

5.1.5 External links

- Blackcoin Website

5.2 Counterparty (technology)

Not to be confused with counterparty.

Counterparty is a financial platform for creating peer-to-peer financial applications on the bitcoin blockchain. The protocol specification and all Counterparty software is open source. The reference client is counterpartyd and a web wallet called Counterwallet showcases all protocol features. The protocol’s native currency, XCP, is the fuel that powers Counterparty. It is slightly deflationary, with approximately 2.6 million XCP having been created by burning Bitcoins in January 2014. Counterparty provides users with the world’s first functioning decentralized digital currency exchange,^[1] as well as the ability to create their own virtual assets, issue dividends, create price feeds, bets and contracts for difference.^[2]

5.2.1 XCP

Counterparty has a native currency called **XCP**. It was originally issued using a provable method called “proof of burn”. This method involves sending bitcoins to a special address that renders the coins permanently unspendable. By avoiding funding during its launch, Counterparty has ensured that developers and users have equal financial opportunities. During January 2014, 2125.63 bitcoins^[3] were sent to 1CounterpartyXXXXXXXXXXXXXXXXXXXXXXXXXXXXUWLpVr^[4] (worth roughly US\$1.8 million at the time).^[5] XCP is used in the Counterparty protocol to create new assets, make bets, and perform callbacks on callable assets. “Since Counterparty can’t function without XCP, it ultimately represents the value of the network.”^[5] Counterparty used proof of burn to issue XCP, instead of a more traditional fund-raising technique for altcoin launches, to keep the initial distribution of funds as fair and decentralized as possible, and to avoid potential legal issues.^{[5][6]}

5.2.2 Assets

With Counterparty, users can create their own currencies inside the bitcoin blockchain. These are separate from bitcoin the currency itself, but exist entirely inside ordinary bitcoin transactions. Tokens can be received, stored, and sent from any bitcoin address to any other. They can also be placed in cold storage. Counterparty tokens are not tied to the BTC balance of any given address. This means that sending/receiving bitcoins has no effect on the balance of tokens. Among other features, Counterparty adds the ability create, send, trade, and pay distributions on assets, in a fully decentralized and trustless manner. While Counterparty has its own internal currency (XCP), trading and creating assets does not require anything apart from regular bitcoin transaction fees.

Many of the features described below can be accessed using the Web-based Counterwallet. Especially casual users and those without a counterparty-cli setup can benefit from the convenience of Counterwallet. Counterparty-issued assets (tokens) can have plain-text or Enhanced Asset Information.

Creating Assets

Counterparty allows users to *issue assets*. An asset that is created within the Counterparty protocol is often called a *user-created token*. User-created tokens are just as real as XCP or even BTC. With the asset issuance function, every user has the ability to create a new currency project inside the bitcoin and Counterparty ecosystem.

You can create two different types of assets:



XCP Symbol

1. **Named:** A unique string of 4 to 12 uppercase Latin characters (inclusive) not beginning with 'A'. Alphabetic tokens carry a one-time issuance fee of 0.5 XCP to discourage spam and squatting. This fee is burned (permanently taken out of circulation). BTC and XCP are the only three-character asset names.
2. **Numeric (Free):** An integer between $26^{12} + 1$ and 256^8 (inclusive), prefixed with A. Numeric assets only require one bitcoin transaction fee to be created.

The different kinds of assets

The most basic kind of asset must specify:

- who is issuing it (source)
- the name of the asset (asset)
- how much of asset is being issued (quantity)
- a description of asset (description)

It is possible to issue more of asset, but, at any one time, there can only be one address which issues asset. With that said, the Counterparty protocol allows source to transfer issuance rights of asset. Moreover, an asset can also be locked, so that there can be no further issuances of it. (See the examples for instructions on how to do this with `withcounterparty-cli`). A description must always be included, even if description is just an empty string; the syntax of an asset *with no description* is `description=""`.

Beyond creating the most basic asset, it is also possible to make assets either *divisible* or *callable*. If an asset is made divisible (or callable) upon its initial issuance, it must always be divisible (or callable) with every issuance thereafter. A divisible user-created asset is, like, bitcoin and XCP, divisible up to 8 decimal places. A callable asset is an asset which the issuer can call back (i.e. repurchase) from its owners at a date (call-date) and for a price (call-price) specified at the initial issuance.

Sending Assets

To send an asset in Counterparty, one must specify:

- who is sending the asset (source)
- what asset source is sending (asset)
- how much of asset source is sending (quantity)
- to whom source is sending quantity of asset (destination)

Paying distributions on assets

It is possible to distribute funds proportionally among asset holders using the distribution function. This feature is also known as dividend payments, depending on their desired purpose. Distributions are paid in in any `distribution_asset` to everyone who holds the asset in proportion to how many units he holds; specifically: Let total equal the total distribution paid out, and quantity be the total amount of asset, then: $quantity-per-unit = total/quantity$

Distributions can be paid out to any assets that you ownership and control over. You can freely select the currency in which distributions are to be paid out: BTC, XCP, or any other user-created asset.

Use-cases

- **Programmable Smart Contracts** - Turing-complete smart contracts scripting is one of the most powerful Counterparty features. Users can write their own custom financial instruments and decentralized applications (Dapp). Counterparty contracts are 100% compatible with Ethereum scripting, and pretty much all contracts can be run on both platforms without code changes.
- **Betting** - Counterparty turns the bitcoin blockchain into a betting platform and prediction market. Oracles can create broadcasts of information, and users can then place bets on these broadcasts. Funds are escrowed automatically by the protocol, and benefit from being stored securely inside the bitcoin blockchain. Funds placed on bets are be provably inaccessible until the bet is resolved or expires. Oracles can set a fee fraction to receive for their betting feeds, providing incentive to run their broadcasts.
- **Tickets & Coupons** - Assets can be used as tickets to a music event, parking tickets, coupons, etc.
- **Token Controlled Access (TCA)** - Token Controlled Access is the idea of granting access to private forums, chatrooms, games, projects or other social media based on the ownership of tokens. Different types of tokens represent different types of membership, and holders of that token can register and/or view the restricted content. To invite new users, smaller fractions of these tokens can be transferred. If the token is indivisible and scarce, it will limit the amount of users others are able to invite. These tokens are also publicly tradable on the DEX and therefore can have a monetary value, and/or one proportional to other types of these tokens.
- **Proof of Publication** - Using broadcasts, users can publish timestamped information onto the bitcoin blockchain. This makes it possible to verify that something has been posted at a certain time, and it cannot be deleted.

- **Crowdfunding** - Counterparty assets can be used for crowdfunding. You can issue a certain amount of assets and sell these to start your project. Due to the high amount of trust involved, it is better to use a Counterparty-based crowdfunding platform which can perform due-diligence on your project. This will provide your users trust, and demonstrate the legitimacy of your project. There is nothing stopping you from doing this on your own, but users may rightfully be suspicious about your project.
- **Derivatives** - You can back Counterparty assets with tangible goods, such as gold.
- **In-game Currency** - To integrate your multiplayer game into the global economy, Counterparty assets can also be used as in-game currency.
- **Altcoin Migration** - If you have an altcoin that seeks to fulfill a specific purpose, but do not wish to continue mining, you can migrate it to Counterparty with proof-of-burn.
- **Verifiable Voting** -Counterparty supports voting through the use of user-created tokens. This means that you can post the terms and options of your vote as a broadcast, and let users vote on its outcome with full transparency by using tokens. If you create a token (EXAMPLE), you can create any other tokens (such as EXAMPLEVOTE) and pay distributions of EXAMPLEVOTE to all holders of EXAMPLE in one single action. Create a distribution payment and choose EXAMPLEVOTE as the currency to distribute. This way, all holders of EXAMPLE will receive EXAMPLEVOTE in the amount you specify. Now all you need are as many different bitcoin addresses as there are choices in your poll. For example: one bitcoin address for yes, one for no. To cast their votes, holders of EXAMPLE can then send the EXAMPLEVOTE they have received to whichever address they agree with. The results of the poll will then be public and verifiable on the bitcoin blockchain, and can be visualized in a block explorer.

5.2.3 Decentralized Exchange (DEX)

Counterparty supports *peer-to-peer asset exchange*: users can trade assets with no middleman and no counterparty risk. The platform upon which trading is done is Counterparty's *decentralized exchange* and the bitcoin blockchain. In what follows trading on the decentralized exchange will be detailed and explained by means of examples. For the purposes of the following use-cases:

- “*ordern*” denotes the *n*th order in time, *give_asset n* denotes the asset being given in the order, etc.
- Sally's creates *order1* and Alice creates *order2*
- *give_asset2 = get_asset1*

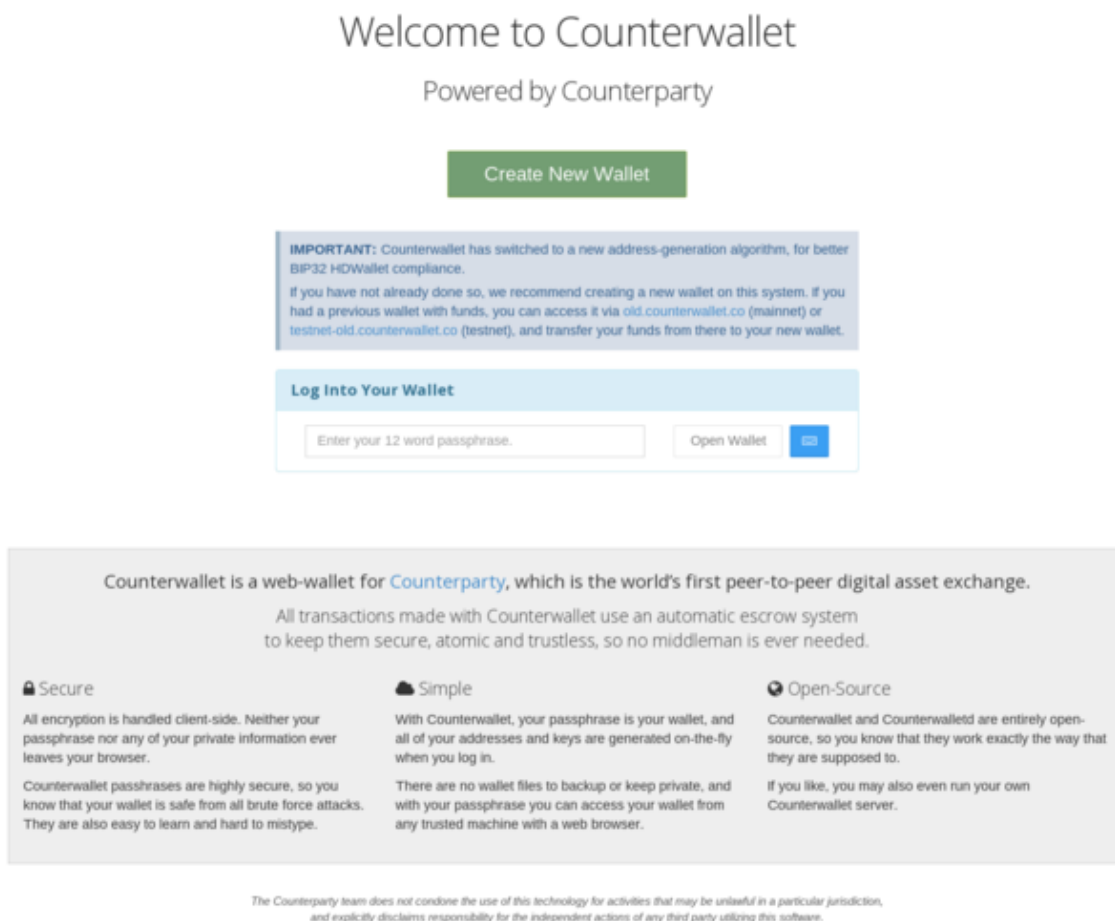
Creating an order

At its most basic level, a trade on Counterparty's decentralized exchange consists of two *orders*, which are *matched* by the protocol. When Sally is constructing her order, she must specify:

- her address (*source1*)
- the asset she will give (*give_asset1*)
- the quantity of *give_asset1* she will give (*give_quantity1*)
- the asset she will get (*get_asset*)
- the quantity of *get_asset1* she will get (*get_quantity*)
- how long before her order expires (*expiration1*)

5.2.4 Software

counterpartyd is the *reference implementation* of the Counterparty protocol, and **Counterwallet** is a deterministic web-wallet frontend to counterpartyd, in which all cryptography is handled client-side. Both are open source and hosted on GitHub.^[7]



Screenshot of Counterwallet Homepage

5.2.5 Notable assets and issuers

- **LTBCoin:**^[8] *Let's Talk Bitcoin*, a podcast about bitcoin, has launched a Counterparty asset called 'LTBCOIN'. LTBCoin is a crypto-rewards system where people who help LTB to be useful are rewarded for their efforts. And it's built on bitcoin! LTBCoin is the proprietary token for the Let's Talk Bitcoin Network. It is the exclusive token accepted for sponsorships. It will provide the user a significant discount in the network wide and ACT-specific e-commerce stores. It can be used in the network for tipping and will generally be useful in every corner of the LTB universe. LTBCoin does not use computational mining. Instead, coins are distributed to the content creators, the community and the platform according to a fixed schedule. After a period of 260 weeks (5 years), all coins will be distributed and no new coins will be created. LTBCoin is a user-defined asset using the Counterparty protocol. LTBCoin can be traded on the Counterparty distributed exchange for XCP or other user-defined assets. The Counterparty Asset ID for LTBCoin is LTBCOIN^{[9][10]}
- **Storj:**^[11] Storj (pronounced: storage) aims to become a cloud storage platform that can't be censored or monitored, or have downtime. Storj is a platform, cryptocurrency, and suite of decentralized applications that allows users to store data in a secure and decentralized manner. It uses blockchain features like a transaction ledger, public/private key encryption, and cryptographic hash functions for security. Furthermore, it will be way cheaper (10x-to-100x), faster, and more secure than traditional cloud storage services. Storj is working hard to solve data security issues with the help of its own web app, MetaDisk, and client app, DriveShare. It is the first decentralized, end-to-end encrypted cloud storage that uses blockchain technology and cryptography to secure online files. There is no need to trust a corporation, vulnerable servers, or employees with your files. Storj completely removes trust from the equation. To best protect your data, files are encrypted client-side on users' computers before they are uploaded. Each file is split up into chunks which are first encrypted and then distributed for storage across the Storj network. The network consists of DriveShare nodes run by users around the world who rent out their unused hard drive space in return for Storjcoin X (SJCX). The decentralized aspect of Storj means there are no central servers to be compromised, and because of the use of client-side

- [5] Alex Brokaw (2014-04-16). “The People Who Burn Bitcoins”. Minyanville. Retrieved 2014-04-26.
- [6] Swanson, Tim (2014). “Chapter 3: Next Generation Platforms”. *Great Chain of Numbers a Guide to Smart Contracts, Smart Property and Trustless Asset Management*. Self-published. Retrieved 2014-04-26.
- [7] Robby Dermody (2014-04-24). “Counterparty: Enabling Decentralization with Insight”. bitcore blog. Retrieved 2014-04-26.
- [8] “Home - LTBCoin - Official token of the Let’s Talk Bitcoin! Network”. *ltbcoin.com*.
- [9] “Counterparty XCP Block Explorer :: Asset Information”. *blockscan.com*.
- [10] Levine, Adam (2014). “LTBCoin and the start of Private Network Tokens”. *LetsTalkBitcoin!*. Adam Levine. Retrieved 2014-03-08.
- [11] “Storj - The Future of Cloud Storage”. *storj.io*.
- [12] “Counterparty XCP Block Explorer :: Asset Information”. *blockscan.com*.
- [13] “What is Storj”. *Storj.io*. Storj Team.
- [14] GetGems Team. “GetGems”. *GetGems - Messaging That Pays. Social Meets Cryptocurrency*.
- [15] “Counterparty XCP Block Explorer :: Asset Information”. *blockscan.com*.
- [16] “FoldingCoin”. *FoldingCoin*.
- [17] “The FoldingCoin White Paper” (PDF). *foldingcoin.net*. FoldingCoin Team. Retrieved 2015.
- [18] “Counterparty XCP Block Explorer :: Asset Information”. *blockscan.com*.
- [19] “Swarm.fund - Revolutionizing Crowdfunding”. *swarm.fund*.
- [20] “How Swarm Plans to Become the Facebook of Crowdfunding”. Retrieved 2015-08-01.
- [21] “Counterparty XCP Block Explorer :: Asset Information”. *blockscan.com*.
- [22] EverdreamSoft. “Spells of Genesis - The First Game that Uses Bitcoin and Blockchain Technology”. *spellsofgenesis.com*.
- [23] EverdreamSoft. “Spells of Genesis - The First Game that Uses Bitcoin and Blockchain Technology”. *www.spellsofgenesis.com*. Retrieved 2015-08-01.
- [24] “Counterparty XCP Block Explorer :: Asset Information”. *blockscan.com*.
- [25] “Tatiana Coin - Tatiana Moroz”. *tatianamoroz.com*.
- [26] “Counterparty XCP Block Explorer :: Asset Information”. *blockscan.com*.
- [27] <https://xcpassets.org/all-assets/>
- [28] “Counterparty XCP Block Explorer :: Home”. *blockscan.com*.
- [29] “CounterpartyChain - Counterparty Blockchain Explorer!”. *counterpartychain.io*.

5.2.8 External links

- Counterparty Project Homepage
- Counterwallet
- Blockscan
- Official Counterparty Forum
- LTBCoin (Counterparty asset)
- Swarm (Counterparty asset)
- SCARAB (Counterparty asset)
- Digital Tangible (Counterparty asset market)

5.3 NEM (cryptocurrency)

For other uses, see [New economy movement](#).

NEM is a peer-to-peer cryptocurrency launched on March 31, 2015^[1] and written in Java.^[2] NEM has a stated goal of a wide distribution model and has introduced new features in blockchain technology in its proof-of-importance (POI) algorithm. NEM also features an integrated P2P secure, multisignature accounts and encrypted messaging system and an [Eigentrust++](#) reputation system. NEM technology is used in the private blockchain Mijin being tested by financial institutions and private companies in Japan.^[3]

5.3.1 History

NEM was started by a Bitcoin Talk forum user called UtopianFuture after having been inspired by [Nxt](#) and wanted to improve upon it. Starting on January 19th, 2014, an open call for participation began on [bitcointalk.org](#).^[4] The goal was to create a community-oriented cryptocurrency from the ground up.^[5]

5.3.2 Development

NEM has gone through extensive open alpha testing starting June 25, 2014, followed by lengthy and comprehensive beta testing starting on October 20, 2014.

The NEM developers are partially pseudonymous.^[6]

5.3.3 Unique features

Code

NEM is a new code base that was written entirely in Java. It uses the POI (proof-of-importance) algorithm instead of POW (proof-of-work). NEM uses a [client-server model](#) where the NIS (NEM Infrastructure Server) runs independent of the NCC (NEM Community Client).^[7]

Reputation System

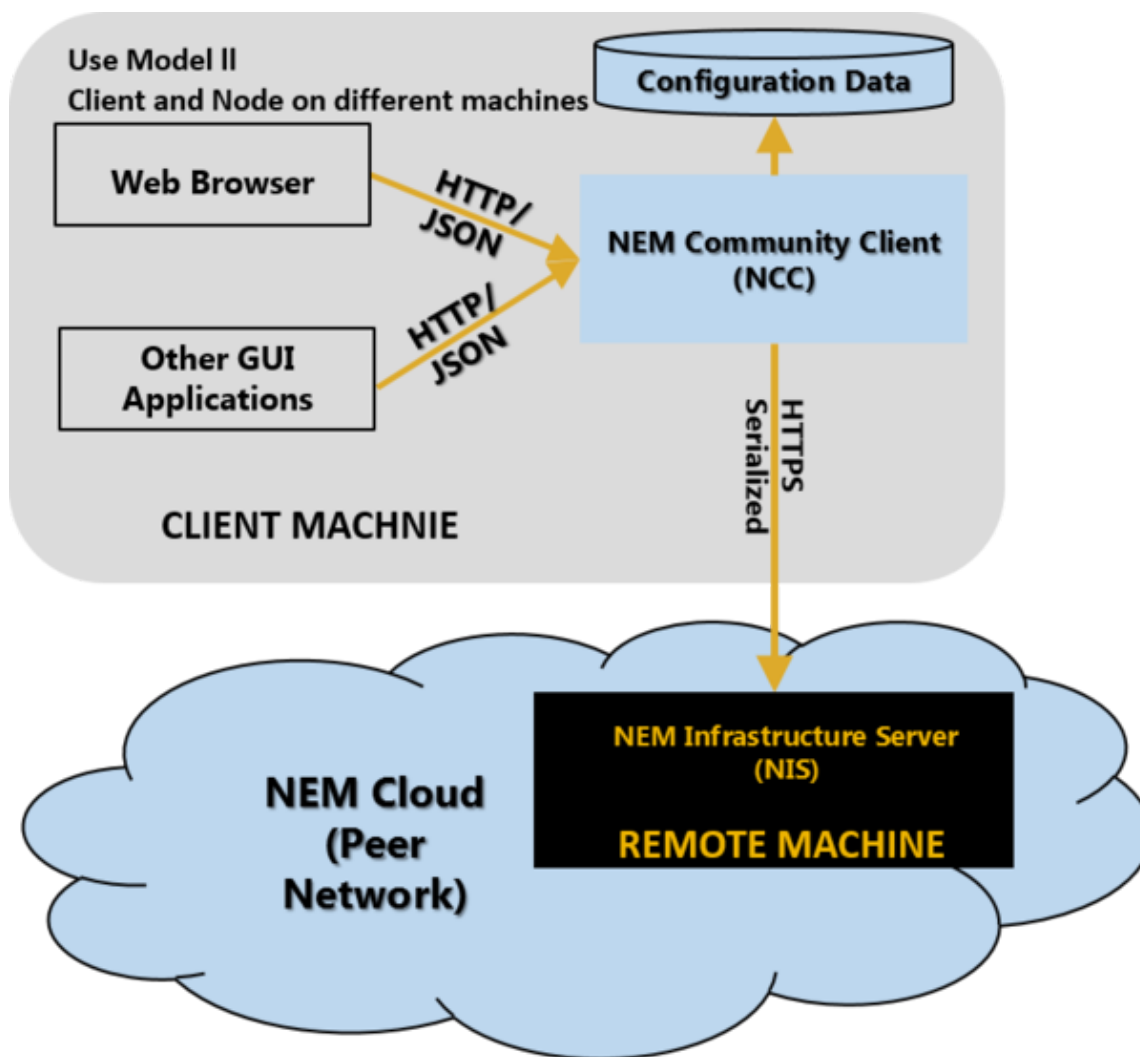
NEM is the first cryptocurrency to employ [Eigentrust++](#) as a reputation system. Whereas other cryptocurrencies might use systems like proof-of-work to ensure the health of the blockchain, NEM does this by monitoring past behavior of nodes within the network. In proof-of-work, the amount of work a node does is used as a measure for its ability to protect the network. But, with [Eigentrust++](#), it is the quality of work that is important. This adds to the NEM network's ability to be run and maintained efficiently.^[8]

Proof-of-Importance

POI is the algorithm used in NEM to time stamp transactions. A NEM user's importance is determined by how many coins they have and the number of transactions made to and from their wallet. POI is different from other initiatives which use a fee-sharing model that does not take into consideration one's overall support of the network. In some proof-of-stake systems a person only needs to have large amounts of coins to form a block; however, in NEM the transaction amount as well as support of the network become a factor. This has been designed to encourage users of NEM to not simply hold NEM but instead actively carry out transactions within the NEM ecosystem.^[9]

Architecture

NEM's design architecture consists of two components. One is the Node server or NEM Infrastructure Server (NIS). The other is the NEM Community Client (NCC). The NIS is connected to the p2p network and acts as a gateway for the NCC. The NCC is basically a client software that includes a wallet. Both the NCC and NIS can be configured



Overview of the NEM Architecture

to run off the same machine. As it is run from the same machine, both the NCC and the NIS will be exposed to the Internet. A second use case is to separate the NIS from the NCC. ^[10]

The NIS can thus be configured to act as an additional layer of protection to the NCC thereby making the NCC reasonably protected within its own confines as it can be made not to connect to the Internet. In addition, one can have the option of putting a firewall between the NCC and the NIS, the NCC is therefore two steps away from the Internet. This means that the NCC can be made to work in stealth mode. This type of modular design makes the NCC insulated from external attacks. It is almost impossible to break into the NCC if the NCC is only connected to the NIS through another firewall. If there is any attack on the wallet, it is almost certain that the attack is from within the network rather than from outside the network. Another feature of this architecture is that the NCC acts as a wallet and can be used on any computer, whereas the NIS represents a node on the NEM network and can be hosted from remote locations. Additionally, the client can be loaded onto any computer and a person's wallet can be reloaded as long as this person has his private key. ^[11]

The NIS can be placed on a Demilitarized Zone (DMZ) in a firewall and therefore itself is protected from the Internet. Hence, there exists many options and configurations. This makes NEM's architecture designed to be secure.

Multisig

NEM implements multisig (short for multi-signature) technology as an integral part of its platform. The benefit of multisig is that it requires more than one user to sign a transaction. Specifically, NEM implements m of n multisig, where $m \leq n$. Put in another way, m out of a total of n signatories must sign a transaction before it can be broadcast

onto the block chain.

Multisig is a technology for enhanced wallet security. Multisig requires that another user or users sign a transaction before it can be broadcast onto the block chain. This means that if one loses the wallet through a hack, no money can be spent unless another wallet (or wallets if m is more than 2) signs it. Multisig also helps protect community-held funds, in that a majority of designated users must agree before a transaction can be spent from a community-held wallet. This is useful, for example, for fundraising or other community-oriented financing in order to prevent one rogue community leader from stealing funds over which he or she has been given control.

Mijin

Mijin is a private blockchain based on NEM technology and utilizing the same APIs. It is being designed to decrease the costs for banking institutions by 90% while at the same time increase security.^[12] It is being tested by Japan's largest trust bank, SBI Sumishin, owned by Sumitomo Mitsui Trust Holdings, to add to their online banking services.^[13] Additionally, Sakura Internet has teamed up with Tech Bureau to offer 6 month free trials of Mijin.^[14] Mijin is also being tested by Infoteria in its enterprise software Asteria.^[15]

5.3.4 External links

- Official website
- Official forum

5.3.5 References

- [1] Beikverdi, Alireza. "NEM Launches, Targets Old Economy with Proof-of-Importance". *Coin Telegraph*. Coin Telegraph. Retrieved 1 April 2015.
- [2] "GitHub - New Economy Movement". *GitHub*. Retrieved 4 January 2015.
- [3] Maras, Elliot. "Japanese Financial Institutions Partner With Technology Startups To Utilize The Blockchain". *Cryptocoinsnews*. Retrieved 21 December 2015.
- [4] utopianfuture. "[ANN] NEM : 4 billions coins". *Bitcoin Forum*. Retrieved 4 January 2015.
- [5] Mikha, Sean. "How I Got \$1500 for Commenting On an Article". *Lets Talk Bitcoin*. Retrieved 4 January 2015.
- [6] Tanzarian, Armand. "An Introduction to the New Economy Movement". *Cointelegraph*. Retrieved 4 January 2015.
- [7] Lombardo, Hans. "NEM Q&A – Original, Tested Blockchain Platform, Proof-of-Importance, "Change the World, Forever" Tech". *allcoinsnews*. Retrieved 9 April 2015.
- [8] Pangburn, DJ. "This Cryptocurrency Doesn't Want to Beat Bitcoin, It Wants to Beat the Economy". *Motherboard*. Retrieved 4 January 2015.
- [9] Beikverdi, Alireza. "Proof-of-Importance: How NEM is Going to Add Reputations to the Blockchain". *Coin Telegraph*. Retrieved 13 March 2015.
- [10] Lombardo, Hans. "NEM Q&A – Original, Tested Blockchain Platform, Proof-of-Importance, "Change the World, Forever" Tech". *allcoinsnews*. Retrieved 9 April 2015.
- [11] Admin. "New Economy Movement (NEM) – Cryptocurrency 2.5". *Cryptoland*. Retrieved 4 January 2015.
- [12] Holmes, B. "Japanese Company, Tech Bureau, Launches Private Blockchain Project". *Bravenewcoin*. Retrieved 21 December 2015.
- [13] Rizzo, Pete. "Japan's SBI Sumishin Building Blockchain Banking Proof-of-Concept". *Coindesk*. Retrieved 21 December 2015.
- [14] Redman, Jamie. "Mijin: 'Offering Blockchains To The World for Free'". *The Bitcoinist*. Retrieved 21 December 2015.
- [15] Asayama, Takao. "Infoteria Announces Collaboration with Private Blockchain Startup Tech Bureau". *prweb*. Retrieved 21 December 2015.

5.4 Nxt

For other uses, see **NXT**.

Nxt is an open source cryptocurrency and payment network launched in November 2013 by anonymous software developer *BCNext*. It uses **proof-of-stake** to reach consensus for transactions - as such there is a static money supply and, unlike bitcoin, no mining. Nxt was specifically conceived as a flexible platform around which to build applications and financial services.^[3] It has an integrated Asset Exchange (comparable to **shares**), messaging system and marketplace. Users can also create new currencies within the system. The last major release enabled **Multisignature** capabilities and a plugin-system for the client.^[4]

Nxt has been covered extensively in the “Call for Evidence” report by **ESMA**,^[5] to which the Nxt community responded in July 2015.^[6]

5.4.1 History

On 28 September 2013 Bitcointalk.org member BCNext created a forum thread announcing the proposed launch of Nxt as a second generation cryptocurrency and asking for small bitcoin donations to determine how to distribute the initial stake. On 18 November 2013 fundraising for Nxt was closed, with 21 BTC raised.^[7] The genesis block was published on 24 November 2013. It revealed that 1,000,000,000 coins had been distributed to 73 stakeholders in proportion to their level of contribution.^[2] The source code was partially released on 3 January. The full source code was released on 1 March 2014 under the **MIT License**.^[8]

5.4.2 Concept

Just as with **bitcoin**, the **blockchain** is at the core of this currency. But Nxt is written completely from scratch^[9] and has departed in several ways from existing cryptocurrencies. Most notably, in one of his founding statements, BCNext asked the community not to consider the **NXT** coin as the important part, but rather to create currencies on top of it^[10] - possibly devaluing the core currency.

- Nxt is coded in **Java**.
- Nxt was the first currency to rely purely on **proof-of-stake** for consensus. Allowing a block creation rate of roughly one minute.^[11]
- The standard client works as a brain-wallet: Instead of storing keys in a wallet file, security works via a secret passphrase. This means it can be accessed from any instance of the Nxt software.

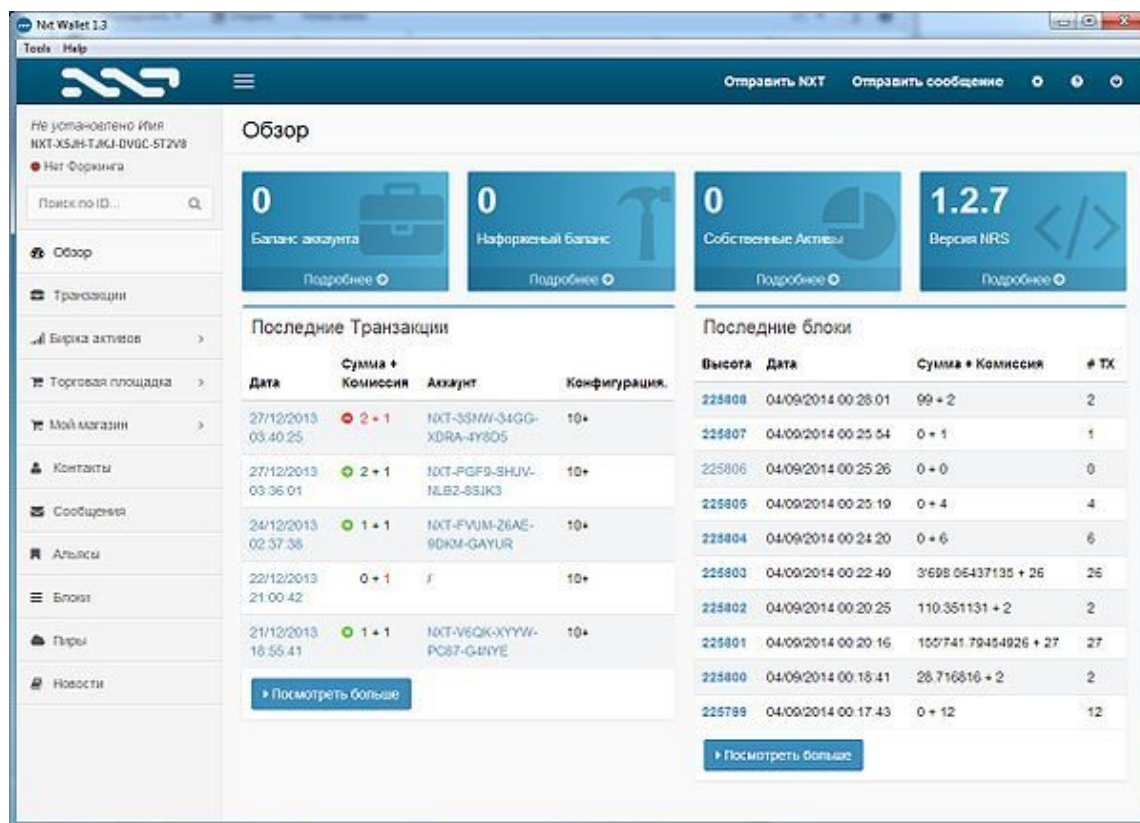
Developer Accessibility

The core structure and the client features are aimed at facilitating external development.

- No centralized service is needed for accessing the API, not even a node run by the developer, since named peers of the network can be directly accessed via API calls.^[12]

Proof-of-Stake Consensus Mechanism

While **bitcoin** uses **hashing power** as **proof** for verifying transactions, Nxt works with the **stake-size** the user owns. Block authors are selected in a practically random manner, with greater amounts of stake increasing the likelihood of adding a block to the chain.^[1] While in the case of **bitcoin** the cost of investing in mining gear serves as an incentive not to attack the network, anyone seeking to attack Nxt would in the process necessarily reduce the value of their personal coin holdings. This effectively avoids the security issue of a miner gaining 51% of the hashing power and attacking the network.^[13]



The standard client is running in web browsers (Russian version pictured).

Forging

Since NXT has an unchanging coin supply, no new units are created for block rewards. Instead the transaction fees are passed on. After owning NXT for about one day (1440 confirmations),^[14] the NXT software will begin to contribute to the block generation process and can potentially earn coins for as long as an account is “unlocked”.

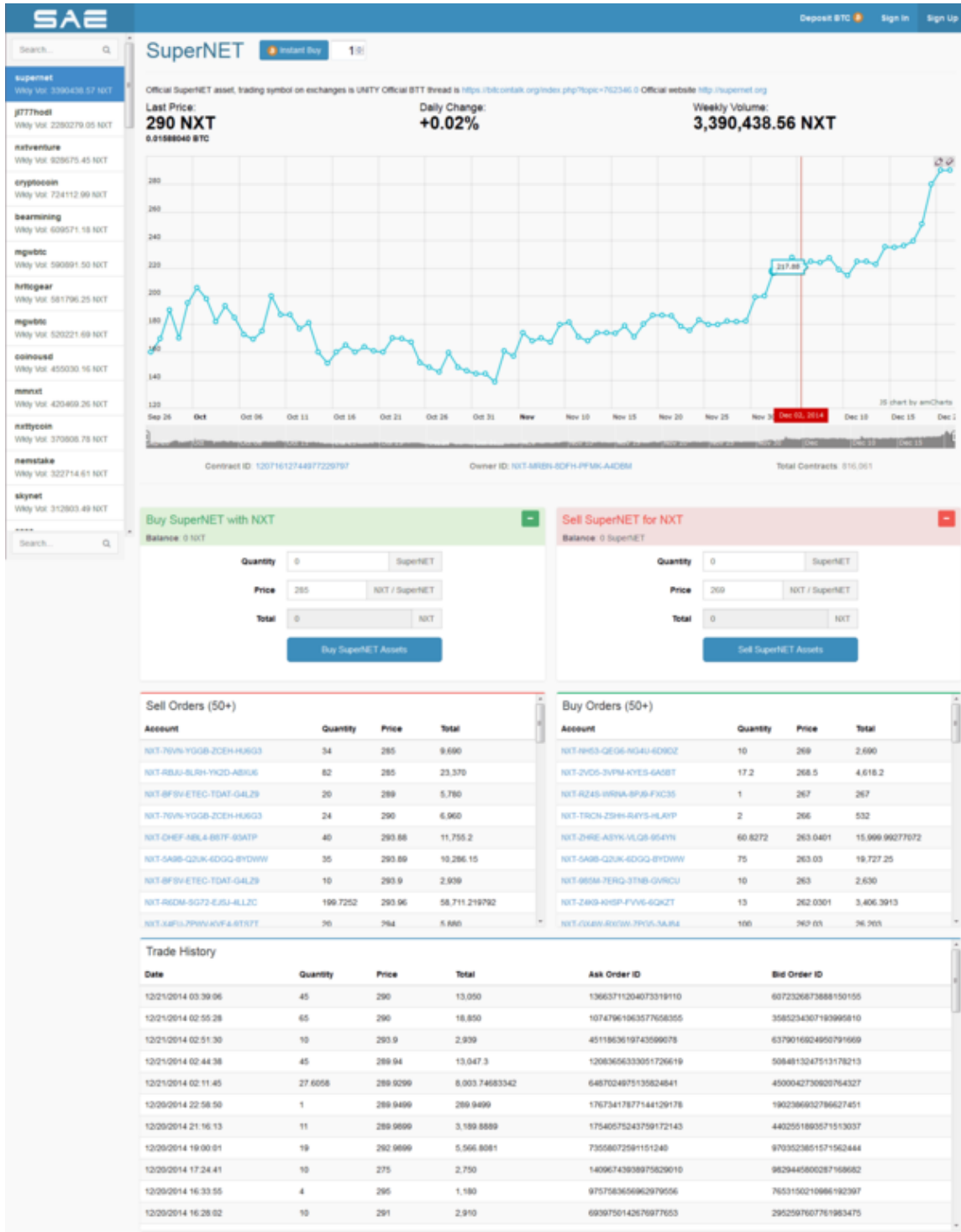
At the moment NXT is open to attack if any account has 51% of the total coin supply that is forging.^[15] As outlined in the founding statements^[10] future versions of NXT will include “transparent forging”, a process which allows the software to predict which accounts will forge upcoming blocks. This is basically done by iterating through all active accounts and seeing which one has the highest “hit”. Transparent forging rapidly increases transaction processing, since the account that will forge the next block is known. Another benefit of this feature is that accounts that are due to forge, but do not, will be penalized by having their forging power temporarily reduced to zero. This raises the threshold for an attack to 90%.^[15] The Proof-of-Stake algorithm requires little computation and energy, and can run on smartphones and small devices like the Raspberry Pi platform.

5.4.3 Features

The core infrastructure of NXT is complex. This adds risks as compared to the more lean bitcoin, but makes it easier for external services to be built on top of the blockchain.^[3]

Asset Exchange

A peer-peer exchange allowing decentralized trading of shares, crypto assets. Since the blockchain is an unalterable public ledger of transactions, the Asset Exchange provides a trading record for items other than NXT. To do this, NXT allows the designation or “coloring” of a particular coin, which builds a bridge from the virtual crypto-currency world to the physical world. The “colored coin” can represent property, stocks/bonds, commodities, or even concepts.^{[16][17]}



Screenshot of the SecureAE Asset Exchange window

Data Storage

Arbitrary Messages enable the sending of encrypted or plain text, which can also function to send and store up to 1000 bytes of data permanently, or 42 kilobytes of data for a limited amount of time. As a result, it can be used to build file-sharing services, decentralized applications, and higher-level Nxt services.^[5]

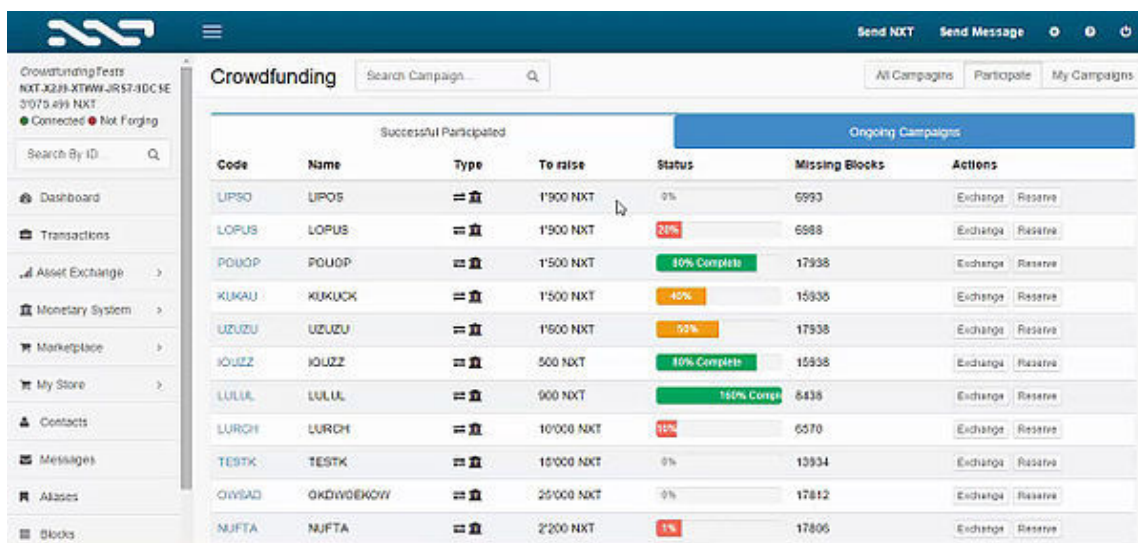
Alias System

The Alias System feature of Nxt essentially allows one piece of text to be substituted for another, so that keywords can be used to represent other things – names, telephone numbers, physical addresses, web sites, account numbers or emails. This would for example allow for a decentralized DNS system similar to Namecoin.^[18]

Voting System

Allowing holders of the currency or Nxt-Assets to vote in a cryptographically proven and externally verifiable way. This can be used for future development decisions, or for shareholder voting. It can also be applied to public elections and community based decision-making.^[4]

Plugin Support



The screenshot shows a web interface for crowdfunding on the Nxt blockchain. The main content is a table titled 'Crowdfunding' with a search bar and navigation tabs for 'All Campaigns', 'Participate', and 'My Campaigns'. The table is divided into 'Successful/Participated' and 'Ongoing Campaigns'. The 'Ongoing Campaigns' section contains the following data:

Code	Name	Type	To raise	Status	Missing Blocks	Actions
LIPSO	LIPOS	==	1'900 NXT	0%	6993	Exchange Reserve
LOPUS	LOPUS	==	1'900 NXT	20%	6888	Exchange Reserve
POLOP	POLOP	==	1'500 NXT	10% Complete	17938	Exchange Reserve
KUKAU	KUKUCK	==	1'500 NXT	40%	16936	Exchange Reserve
UZUZU	UZUZU	==	1'500 NXT	99%	17538	Exchange Reserve
IOUEZ	IOUEZ	==	500 NXT	10% Complete	15538	Exchange Reserve
LULUL	LULUL	==	900 NXT	100% Complete	8438	Exchange Reserve
LURCH	LURCH	==	10'000 NXT	11%	6570	Exchange Reserve
TESTK	TESTK	==	10'000 NXT	0%	13934	Exchange Reserve
OKVSAD	OKDVOEKOW	==	25'000 NXT	0%	17812	Exchange Reserve
NUFTA	NUFTA	==	2'200 NXT	1%	17806	Exchange Reserve

A plugin running on NXT test-net, that will allow easier crowdfunding.

The standard Nxt client supports the installation of plug-ins. This makes it possible for external developers to add features or usability enhancements. The plug-ins are not contained in a sandbox.^[19]

Monetary System

Implemented in version 1.4.8,^[20] the Monetary System allows the creation of currencies on the Nxt blockchain.^{[21][22]} These coins are backed by a specified amount of NXT, which can be redeemed if necessary. The possible properties range widely - including different models of inflation, exchange and the use of Proof-of-Work as distribution system.^[23]

Multi-signature and Phased transactions

The latest client (1.5) supports a method (named *Phasing* for Nxt) for requiring specific conditions for executing a transaction.^[4] Such as approval of multiple accounts or the passage of an interval of time.

5.4.4 Criticism

Nothing at Stake Attacks

It is proposed that one could attack any Proof-of-Stake currency with zero costs.^[24] There are several proposed attack vectors. These include attempting to build blocks in every fork in the network, because doing so costs them almost

nothing and ignoring any fork may mean losing out on the block rewards that would be earned if that fork were to become the chain with the largest cumulative difficulty.

Distribution

Since Nxt had no mining phase, all initial units were released to 73 people through a one-time fund raiser via bitcoins, after the announcement of the NXT project in the bitcointalk-forums by its inventor BCnext.^[25]

User-generated passwords

To access an account, the user types a password or a passphrase from which a private key is calculated, unlike bitcoin, where private keys are typically stored in a wallet file and not directly visible to the user.

5.4.5 3rd Party use

Local Economies

On the 18th of September, Wall Street investor Brian Kelly announced he would be investing in the Nxt based platform Drachmae, which has as its aim the revitalisation of the local economy of the Greek Island Agistri.^[26]

5.4.6 See also

- Cryptocurrency
- Alternative currency
- Crypto asset
- Peer-to-peer computing

5.4.7 References

- [1] "Nxt Whitepaper". Retrieved 2014-03-09.
- [2] "Genesis-Account". *myuxt.info Blockexplorer*. Retrieved 21 December 2014.
- [3] "Nxt Wants to Be a Digital Infrastructure of Everything". *cointelegraph.com*. Retrieved 22 December 2014.
- [4] "NXT Phasing News". *Cointelegraph*. Retrieved 14 June 2015.
- [5] "Call for evidence Investment using virtual currency or distributed ledger technology" (PDF).
- [6] LOPEZ PORTO, Marcos José (2015-07-21). "European Securities and Markets Authority Report" (PDF).
- [7] "NXT Fundraising Over". *bitcointalk.org*. Retrieved 22 December 2014.
- [8] "nxt - source code MIT license". *Bitbucket.org*. Retrieved 21 December 2014.
- [9] "Cryptocurrency News Round-Up: Mt Gox Fire Sale as Jamaica Bobsled Rides Again". *IBTimes*. 2014-02-17.
- [10] "BCNext Founding Statements". *nxtcr.org*. Retrieved 22 December 2014.
- [11] Chepurnoy, Alexander. "Nxt forging algorithm: simulating approach". *scribd.com*. Retrieved 22 December 2014.
- [12] "Nxtpeers API". *nxtpeers.com*. Retrieved 15 January 2015.
- [13] Eyal, Ittay; Gun Sirer, Emin. "Majority is not Enough: Bitcoin Mining is Vulnerable". *Cornell University Library*. Cornell University. Retrieved 22 December 2014.
- [14] "Nxt-Whitepaper (Blocks)". *wiki.nxtcrypto.org*. Retrieved 22 December 2014.
- [15] mthcl (pseudonymous). "The math of Nxt forging" (PDF). *pdf on docdroid.net*. Retrieved 22 December 2014.

- [16] “Crypto 2.0 Roundup: Bitcoin’s Revolution Moves Beyond Currency”. *Coindesk*. Retrieved 25 September 2015.
- [17] “Crypto 2.0 Roundup: Bitcoin’s Revolution Moves Beyond Currency”. Retrieved 25 September 2015.
- [18] “NXT is Powering a Decentralized Voting System and Twitter”. *Cryptocoinsnews*. Retrieved 25 September 2015.
- [19] “Nxt Wants Developers to Unleash Apps Via New Plug-in Store”. *cointelegraph.com*. Retrieved 25 September 2015.
- [20] “Nxt Monetary System NRS client 1.4.8”. *nxter.org*. Retrieved 15 January 2015.
- [21] “Nxt Monetary-System on public testnet”. *nxter.org*. Retrieved 22 December 2014.
- [22] “description of the Monetary System”. *bitbucket.org*. Retrieved 22 December 2014.
- [23] “NXT Monetary System Infrastructure Allows Creation of New Cryptocurrencies On NXT Blockchain”. *Yahoo Finance*. Retrieved 25 September 2015.
- [24] Houy, Nicolas. “It Will Cost You Nothing to ‘Kill’ a Proof-of-Stake Crypto-Currency”. *papers.ssrn.com*. University of Lyon 2. Retrieved 22 December 2014.
- [25] “[ANN] Nxt :: descendant of Bitcoin”. Retrieved 20 May 2014.
- [26] Aitken, Roger. “Brian Kelly Capital Investing In First ‘Fully Deployable’ Digi Currency Ecosystem”. Retrieved 2015-09-19.

5.4.8 External links

- Official website
- Nxt source code on Bitbucket

5.5 Ripple (payment protocol)

For other uses, see Ripple.

Ripple is a real-time gross settlement system (RTGS), currency exchange and remittance network by Ripple. Also called the **Ripple Transaction Protocol (RTXP)** or **Ripple protocol**,^[3] it is built upon a distributed open source Internet protocol, consensus ledger and native currency called **XRP** (ripples). Released in 2012, Ripple purports to enable “secure, instant and nearly free global financial transactions of any size with no chargebacks.” It supports tokens representing fiat currency, cryptocurrency, commodity or any other unit of value such as frequent flier miles or mobile minutes.^{[4][5]} At its core, Ripple is based around a shared, public database or ledger,^[6] which uses a consensus process that allows for payments, exchanges and remittance in a distributed process.^[7] The security of the Ripple consensus algorithm was challenged by rivals in 2014,^[8] with Ripple defending the safety of the system.^[9] As of 2014, Ripple is the second-largest cryptocurrency by market capitalization,^{[10][11]} after bitcoin.^{[12][13][14][15]} Currently implemented by companies such as Fidor Bank, the Ripple protocol has been increasingly adopted by banks and payment networks as settlement infrastructure technology,^[16] with *American Banker* explaining that “from banks’ perspective, distributed ledgers like the Ripple system have a number of advantages over cryptocurrencies like bitcoin,” including price and security.^[17]

5.5.1 History

Early development (2004-2012)

The predecessor to the Ripple payment protocol, Ripplepay, was first developed in 2004 by Ryan Fugger,^{[18][19]} a web developer in Vancouver, British Columbia.^[20] Fugger conceived of the idea after working on a local exchange trading system in Vancouver, and his intent was to create a monetary system that was decentralized and could effectively allow individuals and communities to create their own money. Fugger’s first iteration of this system, RipplePay.com,^[21] debuted in 2005 as a financial service to provide secure payment options to members of an online community via a global network.^{[20][22]}

This led to the conception of a new system by Jed McCaleb of **eDonkey network**,^[23] which was designed and built by Arthur Britto and David Schwartz.^[24] In May 2011 they began developing a digital currency system in which transactions were verified by consensus among members of the network, rather than by the mining process used by **bitcoin**, which relies on **blockchain** ledgers.^[21] This new version of the Ripple system^[20] was therefore designed to eliminate bitcoin's reliance on centralized exchanges, use less electricity than bitcoin, and perform transactions much more quickly than bitcoin.^[20] **Chris Larsen**,^[21] who had previously founded the lending services companies **E-Loan** and **Prosper**, joined the team in August 2012,^[23] and together McCaleb and Larsen approached Ryan Fugger with their digital currency idea. After discussions with long-standing members of the Ripple community, Fugger handed over the reins.^[21] In September 2012 the team co-founded the corporation OpenCoin,^[21] or OpenCoin Inc.^{[23][25]}

OpenCoin and Ripple Labs (2012-2013)

Main article: [Ripple \(company\)](#)

OpenCoin began developing a new payment protocol called the Ripple Transaction Protocol (RTXP) based on Ryan Fugger's concepts.^[21] The Ripple protocol enables the instant and direct transfer of money between two parties.^[26] As such the protocol can circumnavigate the fees and wait times of the traditional correspondent banking system,^{[26][27]} and any type of currency can be exchanged including USD, Euros, RMB, yen, gold, airline miles, and rupees.^[28] To maintain security OpenCoin programmed Ripple to rely on a common ledger that is "managed by a network of independent validating servers that constantly compare their transaction records." Servers could belong to anyone, including banks or market makers.^[26] The company also created its own form of digital currency dubbed XRP in a manner similar to bitcoin, using the currency to allow financial institutions to transfer money with negligible fees and wait-time.^[29]

Among OpenCoin's early investors were^[30] **Andreessen Horowitz** and **Google Ventures**.^[26] On July 1, 2013, XRP Fund II, LLC (now called simply XRP II)^[31] was incorporated as a wholly owned subsidiary of OpenCoin, and headquartered in **South Carolina**.^[31] The following day, Ripple announced its linking of the bitcoin and Ripple protocols via the **Bitcoin Bridge**. The bitcoin Bridge allows Ripple users to send a payment in any currency to a bitcoin address.^{[32][33]} Ripple also developed early partnerships with companies such as **ZipZap**.^[34] On September 26, 2013, OpenCoin Inc. changed its name to **Ripple Labs Inc.**,^[25] with **Chris Larsen** remaining CEO.^[35] On the same day the Ripple reference server and client became free software, released as open source under the terms of the **ISC License**.^[2] Ripple Labs continued as the primary contributors of code to the consensus verification system behind Ripple, which can "integrate with banks' existing networks."^[36] In October 2013, Ripple partnered further with ZipZap, with the relationship called a threat to **Western Union** in the press.^[37]

Focus on banking market (2014-2015)

By 2014 Ripple Labs was involved in several development projects related to the protocol, releasing for example an **iOS** client app for the **iPhone** that allows iPhone users to send and receive any currency via their phone.^{[38][39][40]} This Ripple Client app no longer exists.^[41] In July 2014, Ripple Labs proposed **Codium**, a project to develop a new smart contract system that is "programming language agnostic."^[42]

Since 2013 the protocol has been adopted by an increasing number of financial institutions to "[offer] an alternative remittance option" to consumers.^[43] Ripple allows for cross-border payments for retail customers, corporations, and other banks, and Larsen was quoted stating that "Ripple simplifies the [exchange] process by creating point-to-point and transparent transfers in which banks do not have to pay corresponding bank fees."^[28] The first bank to use Ripple was **Fidor Bank** in **Munich**, which announced the partnership in early 2014. Fidor is an online-only bank based in **Germany**.^[44] That September the **New Jersey**-based **Cross River Bank** and **Kansas**-based **CBW Bank** announced they would be using the Ripple protocol.^[3] By December Ripple Labs began working with global payments service **Earthport**, combining Ripple's software with Earthport's payment services system. Earthport's clients include banks such as **Bank of America** and **HSBC**, and it operates in 65 countries. The partnership marked the first network usage of the Ripple protocol.^[45] In December 2014 alone, the XRP price value rose over 200%, helping Ripple surpass **bitcoin** to become the second biggest crypto-currency, and setting Ripple's market capitalization at close to half a billion.^[46]

In February 2015, **Fidor Bank** announced they would be using the Ripple protocol to implement a new real-time international money transfer network,^[47] and in late April 2015, it was announced that **Western Union** was planning to "experiment" with Ripple.^[37] In late May 2015, **Commonwealth Bank of Australia** announced it would be experi-

menting with Ripple^[48] in relation to intrabank transfers.^[49] Since 2012 representatives of Ripple Labs have professed support for government regulation of the crypto-currency market, claiming that regulations help businesses grow.^[50] On May 5, 2015 FinCEN fined Ripple Labs and XRP II \$700,000 for violation of the *Bank Secrecy Act*,^[31] based on the *Financial Crimes Enforcement Network*'s additions to the act in 2013.^[51] Ripple Labs agreed to remedial steps to ensure future compliance, which included an agreement to only transact XRP and “Ripple Trade” activity through registered *money services businesses* (MSB), among other agreements such as enhancing the Ripple Protocol.^[31] The enhancement won't change the protocol itself, but will instead add AML transaction monitoring to the network and improve transaction analysis.^[51] As of 2015, the current release of Ripple Trade is version 0.2.48-3 and the server (known as rippled) is version 0.24.0.^[1]

5.5.2 Concept

Ripple's website describes the *opensource* protocol as “basic infrastructure technology for interbank transactions – a neutral utility for financial institutions and systems.” The protocol allows banks and non-bank financial services companies to incorporate the Ripple protocol into their own systems, and therefore allow their customers to use the service.^[53] Currently, Ripple requires two parties for a transaction to occur: first, a regulated *financial institution* “holds funds and issues balances on behalf of customers.” Second, “market makers” such as *hedge funds* or currency trading desks provide liquidity in the currency they want to trade in.^[54] At its core, Ripple is based around a shared, public database or ledger that has its contents decided on by consensus.^[6] In addition to balances, the ledger holds information about offers to buy or sell currencies and assets, creating the first distributed exchange.^[53] The consensus process allows for payments, exchanges and *remittance* in a distributed process.^[7] According to the *CGAP* in 2015, “Ripple does for payments what *SMTP* did for email, which is enable the systems of different financial institutions to communicate directly.”^[52]

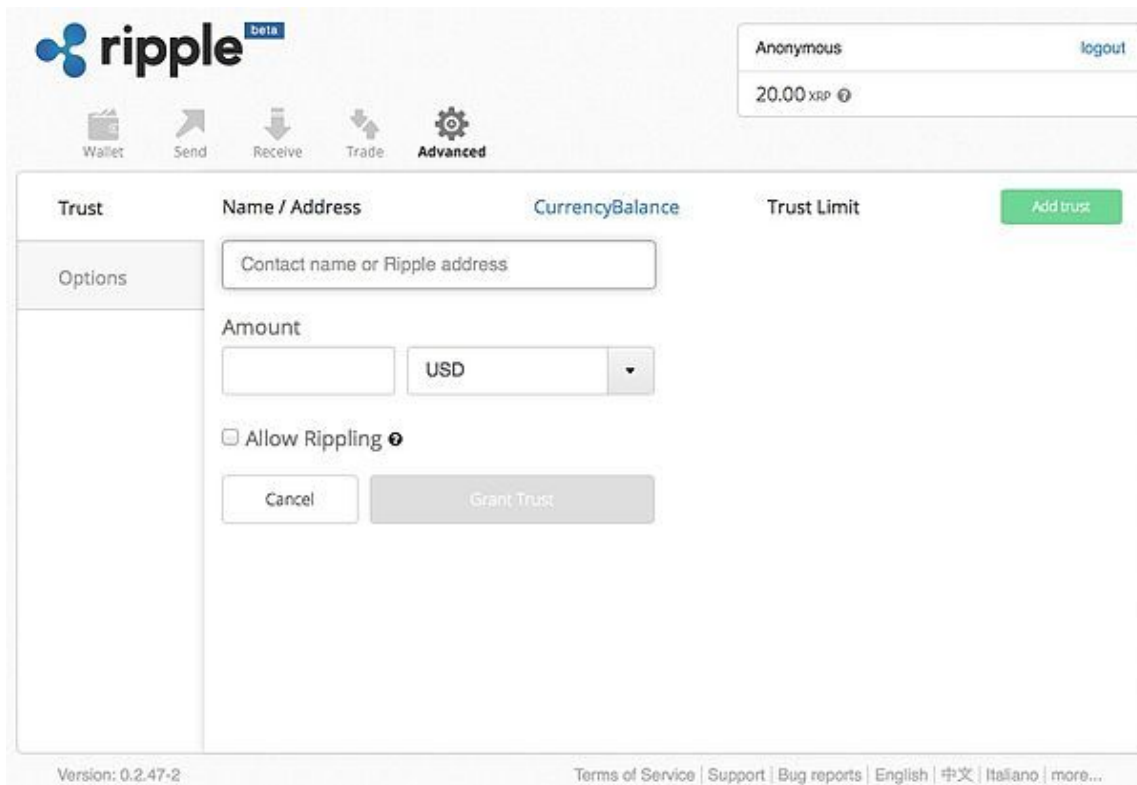
In Ripple, users make payments between each other by using cryptographically signed transactions denominated in either fiat currencies or Ripple's internal currency (XRP). For XRP-denominated transactions Ripple can make use of its internal ledger, while for payments denominated in other assets, the Ripple ledger only records the amounts owed, with assets represented as debt obligations.^[18] As originally Ripple only kept records in its ledger and has no real-world enforcement power, trust was required.^[18] However, Ripple is now integrated with various user verification protocols and bank services.^[55] Users have to specify which other users they trust and to what amount.^[18] When a non-XRP payment is made between two users that trust each other, the balance of the mutual credit line is adjusted, subject to limits set by each user. In order to send assets between users that have not directly established a trust relationship, the system tries to find a path between the two users such that each link of the path is between two users that do have a trust relationship. All balances along the path are then adjusted simultaneously and *atomically*.^[18] This mechanism of making payments through a network of trusted associates is named 'rippling'. It has similarities to the age-old *hawala* system.^[56]

5.5.3 Design features

Gateways

A gateway is any person or organization that enables users to put money into and take money out of Ripple's liquidity pool.^[2] A gateway accepts currency deposits from users and issues balances into Ripple's distributed ledger. Furthermore, gateways redeem ledger balances against the deposits they hold when currency is withdrawn. In practice, gateways are similar to banks, yet they share one global ledger known as the Ripple protocol. Depending on the type and degree of interaction a user has with a gateway, the gateway may have *anti-money laundering* (AML) or *know your customer* (KYC) policies requiring verification of identification, address, nationality, etc. to prevent criminal activity.^[5] Popular gateways as of 2015 included Coinex, Ripple Fox, Panama Bitcoins, Payroutes, Ripple Union, Gold Bullion International, Bluzelle, *Bitstamp*, *SnapSwap*, and *btc2ripple*.^[57]

Trustlines and rippling Users must ‘extend trust’ to the Ripple gateway that holds their deposit. This manual creation of a trustline indicates to the Ripple network that the user is comfortable with the gateway's *counterparty risk*. Furthermore, the user must put a quantitative limit on this trust and create a similar limit for each currency on deposit at that gateway. For example, if a user deposits US\$50 and BTC2.00 at The Rock Trading, the user will have to grant trust of at least that much in both currencies to the gateway for the monies to be available in the Ripple network.^[58] When a user has allowed multiple gateways in the same currency, there is an advanced option to allow



Pictured is the 2014 Ripple user interface that allows for advanced users to add trustlines and “rippling.”

“rippling,” which subjects the user’s balance of that currency to switch (or ripple) between gateways. Though their total balance doesn’t alter, users earn a small transit fee for providing inter-gateway liquidity.^[59]

Creditworthiness Similar to reasons during the **Free Banking Era** in the United States, the value of a currency can vary significantly depending on a gateway’s creditworthiness. A non-profit trade association, the **International Ripple Business Association (IRBA)**, provides unified procedures and disclosure standards for gateways.^{[60][61][62]} As of June 2015, fifteen businesses had met or exceeded the IRBA standards.^{[60][61]}

Consensus ledger

Ripple relies on a common shared ledger, which is a distributed database storing information about all Ripple accounts. The network is “managed by a network of independent validating servers that constantly compare their transaction records.” Servers could belong to anyone, including banks or market makers.^[26] Though the Ripple protocol is freeware,^[2] Ripple Labs continues to develop and promote the Ripple protocol, which confirms financial transactions via a network of distributed servers. Ripple Labs is currently assisting banks in integrating with the Ripple network.^[36] A new ledger is created every few seconds,^[63] and the last closed ledger is a perfect record of all Ripple accounts as determined by the network of servers. A transaction is any proposed change to the ledger and can be introduced by any server to the network. The servers attempt to come to consensus about a set of transactions to apply to the ledger, creating a new ‘last closed ledger’.^[63]

The consensus process is distributed,^[64] and the goal of consensus is for each server to apply the same set of transactions to the current ledger.^[63] Servers continually receive transactions from other servers on the network,^[63] and the server determines which transactions to apply based on if a transaction came from a specified node in the ‘unique node list’ or UNL.^[7] Transactions that are agreed upon by a “supermajority” of peers are considered validated.^[63] If the supermajority isn’t in consensus, “this implies that transaction volume was too high or network latency too great for the consensus process to produce consistent proposals,” and the consensus process is again attempted by the nodes. Each round of consensus reduces disagreement, until the supermajority is reached.^[63] The intended outcome of this process is that disputed transactions are discarded from proposals while widely accepted transactions are included.^[63] While users may assemble their own UNL nodes and have full control over which nodes they trust,

Ripple Labs acknowledges that most people will use the default UNL supplied by their client.^[7]

Ledger security In early 2014,^[65] a rival company called the Stellar Foundation^[66] experienced a network crash.^[8] The company brought in David Mazieres, Stellar's chief scientist and head of Stanford University's secure computing group, to conduct a review of the Stellar consensus system, which was similar to Ripple's. Mazieres declared the Stellar system unlikely to be safe when operating with "more than one validating node,"^[8] arguing that when consensus is not reached, a ledger fork occurs with parts of the network disagreeing over accepted transactions.^[9] The Stellar Foundation afterwards claimed that there was an "innate weaknesses" in the consensus process,^[8] a claim which according to *Finance Magnates*, "Ripple vehemently denied."^[65] Ripple Labs chief cryptographer David Schwartz disputed Mazieres' findings and claimed that Stellar had incorrectly implemented the consensus system, as "the protocol provides safety and fault tolerance assuming the validators are configured correctly."^[9] The company further wrote that after examining Stellar's information, they had concluded "that there is no threat to the continued operation of the Ripple network."^[67]

Use as a payment/forex system

Ripple allows users or businesses to conduct cross-currency transactions^[68] in 3 to 5 seconds.^[53] All accounts and transactions are cryptographically secure and algorithmically verified. Payments can only be authorized by the account holder and all payments are processed automatically without any third parties or intermediaries.^[68] Ripple validates accounts and balances instantly for payment transmission and delivers payment notification with very little latency (within a few seconds).^[69] Payments are irreversible, and there are no chargebacks.^[70] XRP cannot be frozen or seized.^[71] While as of 2014 anyone could open an account on Ripple,^[71] by 2015 identity verification procedures had been implemented.^[55] Ripple's Path-finding Algorithm searches for the fastest, cheapest path between two currencies.^[72] In the case of a user who wants to send a payment from USD to EUR, this could be a "one-hop" path directly from USD to EUR, or it could be a multi-hop path, perhaps from USD to CAD to XRP to EUR.^[73] Path finding is designed to seek out the cheapest conversion cost for the user. As of May 14, 2014, Ripple's gateways allow deposits in a limited number of fiat currencies (USD, EUR, MXN, NZD, GBP, NOK, JPY, CAD, CHF, CNY, AUD), a handful of crypto currencies (BTC, XRP, LTC, NMC, NXT, PPC, XVN, SLL) and a few commodities (gold, silver, platinum).^{[74][75][76]}

The Bitcoin Bridge The bitcoin bridge is a link between the Ripple and bitcoin ecosystems. The bridge makes it possible to pay any bitcoin user straight from a Ripple account without ever needing to hold any of the digital currency. Additionally, any merchant accepting bitcoins has the potential to accept any currency in the world. For example, a Ripple user may prefer to keep money in USD and not own bitcoins. A merchant, however, may desire payment in bitcoin. The bitcoin bridge allows any Ripple user to send bitcoins without having to use a central exchange such as BTC-e to acquire them.^{[33][77]} Bitstamp acts as a gateway for the Ripple payment protocol, among other exchanges.

Privacy

Currently the only simple method for privacy on Ripple Trade is to keep the name of the owner of a wallet secret, as the wallet address (and name if it has one) and its balance and transactions are visible in the ledger.^[78]

Market makers

Any user on Ripple can act as a market maker by offering an arbitrage service such as providing market liquidity, intra-gateway currency conversion, rippling, etc. Market makers can also be hedge funds or currency trading desks. According to the Ripple website, "by holding balances in multiple currencies and connecting to multiple gateways, market makers facilitate payments between users where no direct trust exists, enabling exchanges across gateways."^[79] With a sufficient number of market makers, the path finding algorithm creates a near frictionless market and enables users to seamlessly pay each other via the network in different currencies, without assuming any undesired foreign exchange risk.^[80]

Many such services are offered through a traditional platform of offers to buy or sell one currency for another currency. Bids and asks are aggregated into order books, to create a decentralized exchange. Users can transact with market makers to trade or convert currencies. Ripple's path finding algorithm leverages this functionality to allow users to

send money in one currency and the recipient to receive it in another currency.^[80] For example, a user can pay with USD and the recipient can choose to receive the money in another currency, including bitcoins and XRP.^[80]

Open API

Ripple Labs built the protocol to be friendly to the developer community, and resulting features include an API for its payment network, based on the popular REST API standard. One of the earliest extensions by third-party developers was a Ripple extension to e-commerce platform **Magento**, which enables Magento to read the Ripple public ledger and create an invoice. There has been a Ripple Wallet payment option developed for retail situations as well.^[38]

5.5.4 XRP

XRP is the native currency of the Ripple network that only exists within the Ripple system.^[82] XRP are currently divisible to 6 decimal places, and the smallest unit is called a drop with 1 million drops equaling 1 XRP.^[82] There were 100 billion XRP created at Ripple's inception, with no more allowed to be created according to the protocol's rules.^[83] As such, the system was designed so XRP is a scarce asset with decreasing available supply.^[83] Not dependent on any third party for redemption, XRP is the only currency in the Ripple network that does not entail counterparty risk, and it is the only native digital asset. The other currencies in the Ripple network are debt instruments (i.e. liabilities), and exist in the form of balances.^[2] Users of the Ripple network are not required to use XRP as a store of value or a medium of exchange. Each Ripple account is required, however, to have a small reserve of 20 XRP^[84] (US\$0.38 as of January 28, 2014^[85]). The purpose for this requirement is discussed in the anti-spam section.

XRP distribution

Of the 100 billion created, 20 billion XRP were retained by the creators, who were also the founders of Ripple Labs. The creators gave the remaining 80% of the total to Ripple Labs, with the XRP intended to fund operations.^[83] Ripple Labs also had a short-lived 2013 giveaway of under 200 million XRP (0.002% of all XRP) via World Community Grid.^[86] As of November 30, 2012, 7.2 billion XRP of Ripple Lab's amounts had been distributed,^[87] with some of the amount given to charities such as the Computing for Good initiative, which began offering XRP in exchange for time volunteered on research projects.^[88] As of March 2015, 67% of Ripple Labs's original 80% was still retained by the company,^[83] with Ripple Labs stating that "we will engage in distribution strategies that we expect will result in a stable or strengthening XRP exchange rate against other currencies."^[89] The amount of XRP distributed and their movement can be tracked through the Ripple Charts website.^[90]

XRP as a bridge currency

One of the specific functions of XRP is as a bridge currency,^[73] which can be necessary if no direct exchange is available between two currencies at a specific time,^[91] for example when transacting between two rarely traded currency pairs.^[81] Within the network's currency exchange, XRP are traded freely against other currencies, and its market price fluctuates against dollars, euros, yen, bitcoin, etc. Ripple's design focus is as a currency exchange and a distributed-RTGS, as opposed to emphasizing XRP as an alternative currency.^[81] In April 2015, Ripple Labs announced that a new feature called autobridging had been added to Ripple, with the intent of making it easier for market makers to transact between rarely traded currency pairs. The feature is also intended to expose more of the network to liquidity and better FX rates.^[92]

XRP as an anti-spam measure

When a user conducts a financial transaction in a non-native currency, Ripple charges a transaction fee. The purpose of the fees is to protect against network flooding by making the attacks too expensive for hackers. If Ripple were completely free to access, adversaries could broadcast large amounts of "ledger spam" (i.e. fake accounts) and "transaction spam" (i.e. fake transactions) in an attempt to overload the network. This could cause the size of the ledger to become unmanageable and interfere with the network's ability to quickly settle legitimate transactions. Thus, to engage in trade, each Ripple account is required to have a small reserve of 20 XRP,^[84] (US\$0.38 as of January 28, 2014^[85]), and a transaction fee starting at .00001 XRP (US\$.0000002 as of January 28, 2014^[85]) must be spent for each trade. This transaction fee is not collected by anyone; the XRP is destroyed and ceases to exist.^[93] The

transaction fee rises if the user posts trades at an enormous rate (many thousands per minute), and resettles after a period of inactivity.^[58]

5.5.5 Reception

Since its debut the Ripple protocol has received a fair amount of attention in both the financial and mainstream press. Ripple has recently been mentioned in industry articles by *The Nielsen Company*, the *Bank of England Quarterly Bulletin*, *NACHA*, and *KPMG*, with many of the articles examining Ripple's effect on internationalizing the banking industry.^[94] In April 2015, *American Banker* asserted that "from banks' perspective, distributed ledgers like the Ripple system have a number of advantages over cryptocurrencies like Bitcoin," including security.^[17] Wrote the *Federal Reserve Bank of Boston*, "the adoption of distributed networks, such as Ripple, may help the [banking] industry realize faster processing, as well as greater efficiencies for global payments and correspondent banking."^[94] Writing for *Esquire* about Ripple as a payment network in 2013, Ken Kurson said that "the big financial-service brands ought to feel about Ripple the way the record labels felt about Napster."^[95] *The New York Times* website *Dealbook* points out in 2014 that "(Ripple) is winning something that has proved elusive for virtual currencies: involvement from more mainstream players in the financial system."^[16]

Comparisons to competition

Though Ripple is second in size to bitcoin as a digital currency, many members of the press have described Ripple as an up-and-coming rival to bitcoin. In late 2014, *Bloomberg* called bitcoin a "failing" digital currency, after bitcoin's currency fell 54 percent in value in one year. Ripple was described as a significant competitor, in part because of its real-time international money transfers.^[96] *Bill Gates* supported this outlook and mentioned the Ripple system when asked about bitcoin in 2014, stating "there's a lot that bitcoin or Ripple and variants can do to make moving money between countries easier and getting fees down pretty dramatically. But bitcoin won't be the dominant system."^[97] About Ripple's allowance of any electronic value holder, the Vice President of the *St. Louis Federal Reserve* and professor at *Simon Fraser University*, David Andolfatto, stated in 2014 that "Ripple is a currency-agnostic protocol. Ripple is the winner. It processes anything."^[98] For its creation and development of the Ripple protocol (RTXP) and the Ripple payment/exchange network, the *Massachusetts Institute of Technology (MIT)* recognized Ripple Labs as one of 2014's 50 Smartest Companies in the February 2014 edition of *MIT Technology Review*.^[99]

Reactions to XRP

The reaction to XRP is polarized in the crypto-currency community.^[7] Proponents of bitcoin have criticized XRP for being "pre-mined," as XRP is built directly into the Ripple protocol and requires no mining. Also, Ripple Labs' distribution of the original limited amount of XRP currency has met with a fair amount of controversy,^[65] and in particular the founders' retainment of 20% is seen as a high percentage. However, *Esquire* countered in 2013 that "if that is devious, then so is every company that's ever gone public while retaining the great bulk of its shares."^[95] Much of the controversy was settled after the announcement that the founders^[66] *Jed McCaleb*^[100] and *Arthur Britto*^[66] would be selling their XRP at a mediated rate over several years, "a move that should add stability and restore confidence to the XRP market."^[66] CEO *Chris Larsen* in turn donated 7 billion XRP to the *Ripple Foundation for Financial Innovation*, with the XRP to be "locked up" and donated over time.^[100]

5.5.6 See also

- List of online payment service providers

5.5.7 References

- [1] "Official source code". Github. Retrieved May 14, 2014.
- [2] Buterin, Vitalik (September 26, 2013). "Ripple is officially open source". *Bitcoin Magazine* (Coin Publishing Ltd.). Retrieved January 25, 2014.
- [3] "Two US banks are ready to embrace the Ripple protocol". Gigaom. September 24, 2014. Retrieved 2015-06-09.

- [4] “Ripple Labs Banks \$3.5M for Open-Source Payments System and Virtual Currency”. Dow Jones & Company. Retrieved January 28, 2014.
- [5] Bradbury, Danny (May 27, 2013). “Chris Larsen: Ripple is HTTP for money”. *CoinDesk* (Coindesk Ltd.). Retrieved January 26, 2014.
- [6] “Tech Showcase: Ripple Labs”. Institute of International Finance.
- [7] Liu, Alec. “Beyond Bitcoin: a Guide to the Most Promising Cryptocurrencies”. *Motherboard (beta) blogs*. Vice Media Inc.
- [8] “Safety, liveness and fault tolerance—the consensus choices”.
- [9] “Stellar Network Fork Prompts Concerns Over Ripple Consensus Protocol”.
- [10] “Crypto-Currency Market Capitalizations”. coinmarketcap.com. Retrieved 2014-01-19.
- [11] “LTC/USD alltime - Bitcoin / Altcoin market overview”. cryptocoincharts.info. Retrieved 2014-10-01.
- [12] Simonite, Tom (2013-04-15). “Bitcoin isn't the only cryptocurrency in town”. *MIT Technology Review*. Retrieved April 24, 2013.
- [13] LTCUSD alltime Litecoin US Dollar chart from BTC-e (cryptocoincharts.info)
- [14] Powers, Shawn (March 2012). “Cryptocurrency: Your total cost is 01001010010” (PDF). *Linux Journal* (215): 28–29. Retrieved October 21, 2012.
- [15] BATR (2013-04-17). “Bitcoins risk reward”. *The Market Oracle*. Retrieved April 24, 2013.
- [16] Popper, Nathaniel. “The rush to coin virtual money with real value”. *The New York Times* (The New York Times Company). Retrieved January 26, 2014.
- [17] Todd, Sarah (April 7, 2015). “Banks Can Cherry-Pick the Best Bits from Bitcoin: Report”. *American Banker*. Retrieved 2015-06-16.
- [18] Buterin, Vitalik (February 26, 2013). “Introducing Ripple”. *Bitcoin Magazine*. Retrieved February 6, 2014.
- [19] Deng, Xiaotie; Graham, Fan Chung, ed. (November 29, 2007). *Internet and Network Economics: Third International Workshop, WINE 2007, Proceedings*. Germany: Springer. p. 268. ISBN 978-3-540-77104-3.
- [20] Peck, Morgan (January 14, 2013). “Ripple Could Help or Harm Bitcoin”. *IEEE Spectrum*. Institute of Electrical and Electronics Engineers. Retrieved January 27, 2014.
- [21] Reutzler, Bailey. “Disruptor Chris Larsen Returns with a Bitcoin-Like Payments System”. PaymentSource. Retrieved 18 March 2014.
- [22] Liu, Alec. “Ripple Could Make Bitcoin Great (or Destroy It)”. Motherboard. Retrieved January 27, 2014.
- [23] Grant, Rebecca (April 11, 2013). “OpenCoin raises seed round so ‘anyone in the world can trade any amount of money in any currency’”. *VentureBeat*. Retrieved February 6, 2014.
- [24] Craig, Michael (February 5, 2015). “The Race to Replace Bitcoin”. *Observer*. Retrieved 2015-06-13.
- [25] “Company Overview of Ripple Labs Inc.”. Bloomberg. Retrieved January 27, 2014.
- [26] Andrews, Edmund L. (September 24, 2013). “Chris Larsen: Money Without Borders”. Stanford Graduate School of Business. Retrieved 2015-04-10.
- [27] Bala, Dr. Venkatesh (October 8, 2014). “Lessons in Innovation Leadership: Chris Larsen”. *Nielsen* (The Cambridge Group). Retrieved 2015-06-10.
- [28] Perry, John-David (December 5, 2014). “The Future for Global Value Transfers”. *Fox Business*. Retrieved 2015-06-16.
- [29] Lashinsky, Adam (August 22, 2014). “Isn't one Internet enough?”. *Fortune Magazine*. Retrieved 2015-04-10.
- [30] Shirley, Siluk. “Google Ventures invests in Bitcoin competitor OpenCoin”. CoinDesk. Retrieved 18 March 2014.
- [31] “FinCEN Fines Ripple Labs Inc. in First Civil Enforcement” (PDF).
- [32] “OpenCoin Extends Ripple Network to Include All Bitcoin Merchants and Users”. Yahoo Finance. Retrieved 18 March 2014.

- [33] David, Gilson. "OpenCoin: Ripple users can send payments to bitcoin addresses". CoinDesk. Retrieved March 17, 2014.
- [34] Kharif, Olga. "Ripple Takes on Western Union With Deal to Grow Payments". Bloomberg. Retrieved January 28, 2014.
- [35] "The Future of Money and Bitcoin by Chris Larsen, CEO of OpenCoin". Retrieved February 24, 2015.
- [36] Cooper, Jane (March 11, 2014). "Ripple Labs CEO looks to revolutionise online payments". *The Banker*. Retrieved 2015-04-10.
- [37] Ryan, Philip (April 29, 2015). "Western Union Will Give Ripple a Chance". *Bank Innovation*. Retrieved 2015-06-09.
- [38] Bradbury, Danny. "Ripple Courts Developers, Entrepreneurs With New Initiatives". CoinDesk. Retrieved 18 March 2014.
- [39] "Introducing Ripple Client: the iOS App". *Ripple Blog*. Ripple Labs Inc.
- [40] Kirk, Jeremy. "Apple removes Blockchain, last Bitcoin wallet app, from iOS App Store". PCWorld. Retrieved 18 March 2014.
- [41] Download the Ripple Client - Official site Archived June 4, 2015 at the Wayback Machine
- [42] Cawrey, Daniel (July 21, 2014). "Ripple Labs Unveils Proposal for New Smart Contract System". coindesk. Retrieved 2015-06-09.
- [43] Scully, Matt (September 24, 2014). "Alternative Money Mover Ripple Labs Enters U.S. Banking System". *American Banker*. Retrieved 2015-06-16.
- [44] Bannister, David (September 30, 2014). "Next out of the block". *Banking Technology*. Retrieved 2015-06-09.
- [45] Paul Vigna, Michael Casey (December 4, 2014). "BitBeat: Ripple Partners With Global Payments Service Earthport". *Wall Street Journal*. Retrieved 2015-06-09.
- [46] Wilmoth, Josiah (December 13, 2014). "XRP price rise gives Ripple \$500 million market cap". *CryptoCoinNews*. Retrieved 2015-06-09.
- [47] Reutzel, Bailey (February 23, 2015). "Digital-Only German Bank to Enter U.S. Market, Court Millennials". *American Banker*. Retrieved 2015-06-09.
- [48] Riley, Duncan (June 1, 2015). "CBA signs deal with Ripple for Blockchain settlements, may eventually support Bitcoin". *Silicon Angle*. Retrieved 2015-06-09.
- [49] Merrett, Rebecca (May 27, 2015). "Commonwealth Bank to launch Ripple payments between its subsidiaries". *CIO*. Retrieved 2015-06-05.
- [50] Higgins, Stan (November 3, 2014). "Money20/20 Day 1: Regulators, Finance Giants Forecast Bitcoin's Future". CoinDesk. Retrieved 2015-06-09.
- [51] "What Ripple's Fincen Fine Means for the Digital Currency Industry". *American Banker*. May 6, 2015. Retrieved 2015-06-09.
- [52] "The 'Ripple' Effect: Why an Open Payments Infrastructure Matters". Consultative Group to Assist the Poor. May 1, 2015.
- [53] "Executive Summary for Financial Institutions". ripple.com. Retrieved 2015-06-16.
- [54] Katakam, Arunjay (September 4, 2014). "The evolution of cross-border transfers: new infrastructure for MNO's to increase remittance". GSMA. Retrieved 2015-06-16.
- [55] Trach, Alina (May 27, 2015). "Ripple Trade to Implement Identity Verification Procedures". ripple.com. Retrieved 2015-06-05.
- [56] "Ripple Explained: Medieval Banking with a Digital Twist".
- [57] "Gateway Information". ripple.com. Retrieved 2015-06-16.
- [58] John, Light. "Decentralized Exchange for Fun and Profit". Let's Talk Bitcoin. Retrieved January 26, 2014.
- [59] Tong, Anna. "Understanding trust lines". Ripple Labs. Retrieved February 2, 2014.
- [60] "Ripple Gateways". IRBA. Retrieved January 27, 2014.
- [61] "Public Disclosure Standards". International Ripple Business Association. Retrieved May 14, 2014.
- [62] "International Ripple Business Association". ZoomInfo. Retrieved May 14, 2014.

- [63] Britto, Arthur. "The Ripple Ledger Consensus Process". *ripple.com*. Retrieved 2015-05-09.
- [64] "The Science of Trust".
- [65] Pick, Leon (April 23, 2015). "Ripple orders freeze". *Finance Magnates*. Retrieved 2015-06-09.
- [66] Carney, Michael (August 15, 2014). "Ripple settles with estranged founder Jed McCaleb, outlining a metered sale of his XRP holdings". *Pando.com*. Retrieved 2015-06-09.
- [67] Thomas, Stefan (December 7, 2014). "Why the Stellar Forking Issue Does Not Affect Ripple". *ripple.com*. Retrieved 2015-06-05.
- [68] "Payment Network". Ripple Labs. Retrieved February 2, 2014.
- [69] Simonite, Tom (April 11, 2013). "Big-name investors back effort to build a better Bitcoin". *MIT Technology Review*. Retrieved January 26, 2014.
- [70] Schwartz, Ariel. "Bitcoin 2.0: Can Ripple Make Digital Currency Mainstream?". *Fast Company*. Retrieved February 2, 2014.
- [71] McGarvey, Robert. "'Ripple' is the New Bitcoin: Adventures in Virtual Currency". *The Street*. Retrieved February 2, 2014.
- [72] Bradbury, Danny. "Chris Larsen: Ripple is HTTP for money". *CoinDesk*. Retrieved February 2, 2014.
- [73] "Bridge Currency". *Ripple.com*. Retrieved 2015-06-16.
- [74] "Grid". *RippleCharts*. Archived from the original on 10 February 2014. Retrieved January 27, 2014.
- [75] "Company Summary". *Peercover*. Retrieved January 27, 2014.
- [76] Southurst, Jon. "Bullion Exchange Brings Ripple into the Physical World". *CoinDesk*. Retrieved February 2, 2014.
- [77] Bailey, Reutzel. "Ripple Network Adds Currency Conversion for Bitcoin Payments". *PaymentsSource*. Retrieved March 17, 2014.
- [78] "How does Ripple handle privacy?". *ripple.com*. Retrieved October 31, 2014.
- [79] "Market Makers". *Ripple.com*. October 16, 2014. Retrieved 2015-06-16.
- [80] Spaven, Emily. "Online payment network Ripple Labs receives \$3.5m in new funding". *CoinDesk*. Retrieved January 27, 2014.
- [81] "Math Based Currency". *Ripple.com*. Retrieved 2015-06-16.
- [82] "Ripple". *Github*. Retrieved January 28, 2014.
- [83] "XRP Distribution". *Ripple Labs*. Retrieved February 24, 2015.
- [84] "Proposed change to Ripple reserve requirement". *Ripple Blog*. Ripple Labs Inc.
- [85] "Your resource for live Ripple (XRP) exchange rates". *Digigold Pty. Ltd*. Retrieved January 28, 2014.
- [86] "Ripple Forum • View topic - [OFFICIAL] We're moving the giveaway out of beta". Retrieved February 24, 2015.
- [87] Jackson, Brian (January 21, 2014). "Beyond Bitcoin: Top 5 cryptocurrencies by market cap". *IT Business Canada*. IT World Canada Inc.
- [88] Bradbury, Dan. "Ripple Labs now taking cash payments following deal with ZipZap and SnapSwap". *CoinDesk*. Retrieved February 2, 2014.
- [89] "XRP Distribution". *Ripple Labs website*. Ripple Labs Inc.
- [90] "Network Feed". Ripple Labs. Retrieved January 28, 2014.
- [91] King, Steve. "Missed Bitcoin? No Worries.". *Netswitch Technology Management*. Retrieved January 27, 2014.
- [92] Liu, Alec (April 27, 2015). "rippled Feature Update: NuDB and Autobridging". *Ripple Blog*. Retrieved 2015-06-16.
- [93] Teague, Solomon. "First Bitcoin, now Google-backed Open Coin". *EuroMoney*. Retrieved February 2, 2014.
- [94] "Industry Perspectives: Ripple Inclusions". *ripple.com*. Retrieved 2015-06-16.

- [95] Kurson, Ken (November 27, 2013). “The true value of Bitcoin and Ripple”. *Esquire Blogs* (Hearst Communications, Inc.). Retrieved January 26, 2014.
- [96] Kharif, Olga (December 15, 2014). “Bitcoin Bears Say Told-You-So as Digital Currency Falls”. *Bloomberg*. Retrieved 2015-06-16.
- [97] Higgins, Stan (January 22, 2015). “Bill Gates: Bitcoin Alone Won't Solve Global Payments Challenges”. *CoinDesk*. Retrieved 2015-06-16.
- [98] Cawrey, Daniel. “Federal Bank VP: Bitcoin Threat Means Banks Must ‘Adapt or Die’”. *CoinDesk*. Retrieved May 14, 2014.
- [99] Bergstein, Brian. “50 Smartest Companies”. *MIT Technology Review*. Retrieved March 12, 2014.
- [100] Long, Monica (August 14, 2014). “Settlement of Jed's XRP”. *Official Ripple Forum*. Retrieved 2015-06-16.

5.5.8 Further reading

- “Ripple Could Make Bitcoin Great (or Destroy It)”. *Motherboard*. January 23, 2013.
- “Ripple Labs Unveils Proposal for New Smart Contract System”. *CoinDesk*. July 21, 2014.
- “Isn't one Internet enough?”. *Fortune Magazine*. August 22, 2014.

5.5.9 External links

- Ripple.com

5.6 Stellar (payment network)

Stellar is an open source protocol for value exchange. It was founded in early 2014 by Jed McCaleb and Joyce Kim, its board members and advisory board members include Keith Rabois, Patrick Collison, Matt Mullenweg, Greg Stein, Joi Ito, Sam Altman, Naval Ravikant and others.^{[1][2][3][4][5][6]} The Stellar protocol is supported by a nonprofit, the Stellar Development Foundation. The Foundation's mission is to expand financial access and literacy worldwide.^{[7][8][9][10][11][12]} At launch, Stellar was based on the [Ripple protocol](#). After systemic problems with the existing consensus algorithm were discovered, Stellar created an updated version of the protocol with a new consensus algorithm, based on entirely new code. The code and whitepaper for this new algorithm were released in April 2015, and the upgraded network went live in November 2015.^{[13][14][15][16][17][18][19][20]}

5.6.1 Design

Stellar is an open source protocol for value exchange.^[21] Servers run a software implementation of the protocol, and use the internet to connect to and communicate with other Stellar servers, forming a global value exchange network. Each server stores a record of all “accounts” on the network. These records are stored in a database called the “ledger”. Servers propose changes to the ledger by proposing “transactions”, which move accounts from one state to another by spending the account's balance or changing a property of the account. All of the servers come to agreement on which set of transactions to apply to the current ledger through a process called “consensus”. The consensus process happens at a regular interval, typically every 2 to 4 seconds. This keeps each server's copy of the ledger in sync and identical.^{[22][23][24][24]}

5.6.2 Real-world Applications of Stellar

Several nonprofits and businesses are implementing Stellar as financial infrastructure, particularly in the developing world. One such example is [Praekelt Foundation](#), which will be integrating Stellar into Vumi, its open-source messaging app, to let young girls in Sub-Saharan Africa save money in airtime credits.^{[25][26][27][28]}

Oradian, a cloud-based banking software company, also plans to use the Stellar network to connect microfinance institutions (MFIs) in Nigeria.^{[29][30]}

5.6.3 Stellar Consensus Protocol

The white paper and code for the Stellar Consensus Protocol (SCP) were released on April 8, 2015. The white paper introduces federated Byzantine agreement (FBA), a new approach to consensus for which SCP is the first construction. FBA relies on quorum slices, in which each node chooses which other nodes to trust, for system robustness. Together, quorum slices determine system-level quorums. SCP allows open membership.^{[15][17] [31][32][33]}

5.6.4 References

- [1] Michael Casey; Paul Vigna (31 July 2014). "Mt. Gox, Ripple Founder Unveils Stellar, a New Digital Currency Project". *Wall Street Journal*. Retrieved 3 September 2014.
- [2] Cade Metz; Marcus Wohlsen (6 August 2014). "New Digital Currency Aims to Unite Every Money System on Earth". *Condé Nast*. Retrieved 3 September 2014.
- [3] Roberto Baldwin (1 August 2014). "What you need to know about Stellar, the new open-source solution to international currency exchange". *The Next Web*. Retrieved 23 April 2015.
- [4] Michael del Castillo (27 February 2015). "Matt Mullenweg: bitcoin only used twice a week in 2014, offers free subscriptions if you do". *Upstart Biz Journal*. Retrieved 20 November 2015.
- [5] Michael del Castillo (5 August 2014). "Stripe takes on bitcoin with rival digital currency Stellar". *The Irish Times*. Retrieved 20 November 2015.
- [6] Mario Cotillard (5 August 2015). "Digital Currency Startup Stellar Adds Ex-Stripe CTO Greg Brockman To Board". *Brave New Coin*. Retrieved 20 November 2015.
- [7] Jillian D'onfro (31 July 2014). "PayPal's Cofounder Is Supporting A New Non-Profit That Will Tackle The Vision PayPal 'Never Accomplished'". *Business Insider*. Retrieved 23 April 2015.
- [8] Kim-Mai Cutler (31 July 2014). "Stripe Backs Non-Profit Decentralized Payment Network Stellar, From Mt. Gox's Original Creator". *TechCrunch*. Retrieved 23 April 2015.
- [9] JP Mangalindan (31 July 2014). "New Bitcoin challenger launches". *Fortune*. Retrieved 23 April 2015.
- [10] "Stellar Mandate". 31 July 2014. Retrieved 23 April 2015.
- [11] "Certificate of incorporation of Stellar Development Foundation Non-stock Corporation" (PDF). Retrieved 23 April 2015.
- [12] Jacques Coetzee (5 May 2015). "Could Stellar be the answer to enable financial inclusion around the globe?". *Memeburn*. Retrieved 20 November 2015.
- [13] Joyce Kim; (December 4, 2014). "Safety, liveness and fault tolerance—the consensus choices". <http://stellar.org>. Stellar Development Foundation. Retrieved January 14, 2015. External link in |website= (help)
- [14] Cade Metz (8 April 2015). "An Algorithm to Make Online Currency as Trustworthy as Cash". *WIRED*. Condé Nast. Retrieved 23 April 2015.
- [15] Stan Higgins (14 April 2015). "Jed McCaleb Talks Stellar's New Protocol for Consensus". *Coin Desk*. Retrieved 23 April 2015.
- [16] "Stellar Core". *Github*. Retrieved 14 September 2015.
- [17] David Mazieres (14 July 2015). "Stellar Consensus Protocol White Paper" (PDF). <http://stellar.org>. Stellar Development Foundation. Retrieved 14 September 2015. External link in |website= (help)
- [18] Stan Higgins (9 December 2014). "Stellar Network Fork Prompts Concerns Over Ripple Consensus Protocol". *Coin Desk*. Retrieved 23 April 2015.
- [19] Hans Lombardo (5 November 2015). "Stellar Releases Major Upgrade that Runs Faster, Uses Less Memory & Stores Data Better". *All Coin News*. Retrieved 20 November 2015.
- [20] Yessi Bello Perez (8 October 2015). "Stellar Now Open to Developers Following Network Upgrade". *Coin Desk*. Retrieved 20 November 2015.
- [21] "Stellar.org". Retrieved January 14, 2015.
- [22] "How it works". Retrieved January 14, 2015.

- [23] Tom Simonite (8 April 2015). “A New Competitor for Bitcoin Aims to Be Faster and Safer”. MIT Technology Review. Retrieved 20 November 2015.
- [24] Giulio Prisco (17 April 2015). “The New Stellar Consensus Protocol Could Permit Faster and Cheaper Transactions”. Bitcoin Magazine. Retrieved 20 November 2015.
- [25] Biz Carson (5 February 2015). “Stellar, South African nonprofit to bring digital savings to young girls”. GigaOm. Retrieved 23 April 2015.
- [26] Leo Mirani (6 February 2015). “Platforms, not products, are the way to bring financial services to the poor”. Quartz. Retrieved 23 April 2015.
- [27] Tom Simonite (20 February 2015). “Bitcoin-Inspired Digital Currency to Power Mobile Savings App”. MIT Technology Review. Retrieved 23 April 2015.
- [28] Hans Lombardo (2 February 2015). “Non-Profit Foundation Uses Stellar Protocol to Improve Economic Security of South African Girls”. All Coins News. Retrieved 23 April 2015.
- [29] Karen Webster (2 March 2015). “Stellar and Solving the Unexpected Tragedy of the Financial System”. PYMENTS.com. Retrieved 23 April 2015.
- [30] Paul Vigna (28 February 2015). “Stellar Takes a Step Into the Microfinance World”. Wall Street Journal. Retrieved 23 April 2015.
- [31] Cade Metz (8 April 2015). “An Algorithm to Make Online Currency as Trustworthy as Cash”. *WIRED*. Condé Nast. Retrieved 23 April 2015.
- [32] “Stellar Core”. *Github*. Retrieved 23 April 2015.
- [33] Tom Simonite (8 April 2015). “A New Competitor for Bitcoin Aims to Be Faster and Safer”. MIT Technology Review. Retrieved 23 April 2015.

5.6.5 Other websites

- Stellar Foundation

Chapter 6

The technology

6.1 Block chain (database)

A **block chain** or **blockchain** is a permissionless distributed database based on the bitcoin protocol^[1] that maintains a continuously growing list of transactional data records hardened against tampering and revision, even by operators of the data store's nodes. The initial and most widely known application of the block chain technology is the public ledger of transactions for bitcoin^[2] which has been the inspiration for similar implementations often known as altchains.^[3]

6.1.1 Name

The block chain is primarily tamper resistant through timestamping the hash of batches of recent valid transactions into “blocks”, proving that the data must have existed at the time. Each block includes the prior timestamp, forming a chain of blocks, with each additional timestamp reinforcing the ones before it,^[1] thus giving the database type its name. Each block chain record is enforced cryptographically and hosted on machines working as data store nodes extending this validation to the network as a whole.^[4]

6.1.2 Basic principles

The core advantages of the block chain architecture include the following:

- The ability for a significant number of nodes to converge on a single consensus of the most up-to-date version of a large data set such as a ledger, even when the nodes are run anonymously, have poor connectivity with one another, and have operators who may be dishonest or malicious (see Sybil attack).
- The ability for any node that is well-connected to other nodes to determine, with a reasonable level of certainty, whether a transaction does or does not exist in the confirmed data set (see consistency).
- The ability for any node that creates a transaction to, after a certain period of confirmation time, determine with a reasonable level of certainty whether the transaction is valid, able to take place, and become final (i.e. that there were no conflicting transactions confirmed into the block chain elsewhere that would make the transaction invalid, such as the same currency units “double-spent” somewhere else).
- A prohibitively high cost to attempt to rewrite or alter any transaction history.
- An automated form of resolution that ensures that conflicting transactions (such as two or more attempts to spend the same balance in different places) never become part of the confirmed data set.

A block chain implementation consists of two kinds of records: transactions and blocks. Transactions are the actual data to be stored in the block chain, and blocks record and confirm when and in what sequence transactions became journaled as a part of the block chain database. Transactions are created by participants using the system in the normal course of business and blocks are created by users known as “miners” who use specialized software or equipment

designed specifically to create blocks. In the case of cryptocurrencies, a transaction is created anytime someone sends cryptocurrency to another.

Users of the system create transactions which are loosely passed around from node to node on a **best-effort** basis. The definition of what constitutes a valid transaction is based on the system implementing the block chain. In cryptocurrency applications, a valid transaction is one that is properly digitally signed, spends one or more unspent outputs of previous transactions, and the sum of transaction outputs does not exceed the sum of inputs.

Meanwhile, miners attempt to create blocks that confirm and incorporate those transactions into the blockchain. In a cryptocurrency system such as bitcoin, miners are incentivized to create blocks in order to collect two types of rewards: a pre-defined per-block award, and fees offered within the transactions themselves, payable to any miner who successfully confirms the transaction.

6.1.3 Decentralisation

Every **node** in a decentralized cryptocurrency has a complete or partial copy of the block chain. This avoids the need to have a centralized database that other systems, such as PayPal, require.^[5] Whereas a conventional **ledger** records the transfers of actual **bills** or **promissory notes** that exist **apart from it**, the block chain is the only place that cryptocurrency can be said to exist, in the form of unspent outputs of transactions.^{[6]:ch. 5}

Transactions of the form *payer X sends Y currency to payee Z* are broadcast to this network using software applications. Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes.^{[6]:ch. 8}

Cryptocurrencies use various timestamping schemes, such as **proof-of-work**, to avoid the need for a trusted third party to timestamp transactions added to the block chain. This avoids anyone easily **double-spending** the currency.^[7]

6.1.4 Token-less block chain debate

There is an ongoing^[8] debate^{[9][10]} as to whether a blockchain-like system without a native token can still be considered a blockchain^{[11][12]}. Some have argued that token-free block chains serve as a distributed version of **multiversion concurrency control** (MVCC) in databases.^[13] Just as MVCC prevents two transactions from modifying a single row in a database, block chains prevent two transactions from spending a single output in a block chain.

Others have interpreted blockchains' function in a different way, arguing that blockchains are more akin to **finite state machine** automata "where the state of the system is updated sequentially, via atomic transitions (transactions) that are replicated across every machine, in order."^[14]

6.1.5 Data storage

Cryptocurrencies use block chains to timestamp transactions to prevent double-spending.

The bitcoin block chain can also be used as a **trusted timestamp** for arbitrary messages, not just transaction information. Various 3rd party application services store messages directly in the block chain, so anyone who has the block chain can read the message.^{[15][16][17][18]} Bitcoin core developer **Mike Hearn** among others have discouraged embedding large messages in the **bitcoin block chain**, criticizing it as "bloat".^{[19][20][21]}

Other applications store a hash value in the block chain, demonstrating data existence and confirming data integrity without revealing actual data and without bloating the block chain.^{[22][23]} This extra information in the block chain can be used to implement "colored coins" or side chains to support functionality such as **smart contracts**.

6.1.6 Bitcoin sidechain implementations

The **bitcoin network** uses the original bitcoin block chain based on **proof of work**.

Sidechains^[24] are private or public networks that may or may not be based on the bitcoin protocol, and are isolated from the blockchain allowing workflow and functionality to exist in confinement until confirmation on the blockchain is required or desired, at which point bidirectional transferability is supported. These systems work in conjunction with the blockchain. Examples are

- Liquid^[25] - Exchange sidechain from Blockstream
- ChromaWay - Sidechain platform for colored coins
- DIONS - Digital I/O sidechain concept for identity
- tØ (tee-zero) - SEC approved sidechain developed by Overstock.com

6.1.7 Alternative chain designs

Networks running software based on the bitcoin protocol but using alternative cryptocurrency tokens (known as altcoins)^[3] or implementations which are simply database designs in the classical sense exist. These newer designs generally provide additional features or functionality which earlier cryptocurrency designs such as bitcoin's did not. Developments from the first implementation, bitcoin, have built additional features for performance, anonymity, storage and smart contracts.^[26] Starting with a strong focus on financial applications, uses of blockchain technology are progressively extending to many new sectors of activities, including the creation of decentralized applications and collaborative organisations that eliminate a middleman.^[27] Notable designs include:

- Namecoin – Cryptocurrency merge-mined with bitcoin possessing the ability to store data within a chain
- Mastercoin – Cryptocurrency metaprotocol to bitcoin with the ability to process various transactions
- Peercoin – Cryptocurrency incorporating the proof of stake in its consensus model
- Ethereum – Cryptocurrency supporting storage of turing-complete smart contracts at specified addresses on its blockchain, with a 15 second block time
- Billon - Regulated “cryptocash” blockchain solution as digital cash for governmental fiat currencies
- Swarm and Koinify - decentralized crowdfunding
- Synereo - synchronous and asynchronous communication
- LaZooz - decentralized real-time ride sharing

6.1.8 See also

- Bitcoin network
- Colored coins

6.1.9 References

- [1] Satoshi Nakamoto (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System” (PDF). Bitcoin.org. Retrieved 31 October 2008.
- [2] Antonopoulos, Andreas (December 2014). *Mastering Bitcoin - Unlocking Digital Cryptocurrencies*. O'Reilly Media. p. <http://chimera.labs.oreilly.com/books/1234000001802/ch02.html>. ISBN 1-4493-7403-4.
- [3] “Blockchains and the Internet of Things”. Postscapes.
- [4] “How does Bitcoin work?”. Bitcoin.org. Retrieved 20 May 2015.
- [5] Jerry Brito and Andrea Castillo (2013). “Bitcoin: A Primer for Policymakers” (PDF). *Mercatus Center*. George Mason University. Retrieved 22 October 2013.
- [6] Andreas M. Antonopoulos (April 2014). *Mastering Bitcoin. Unlocking Digital Crypto-Currencies*. O'Reilly Media. Retrieved 23 October 2014.
- [7] 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”

- [8] “It’s All About the Blockchain - Money and State”. *Money and State*. Retrieved 2015-11-02.
- [9] Reutzel, Bailey. “A Very Public Conflict Over Private Blockchains”. *Payments Source*. SourceMedia.l title=Blockchain Conflict
- [10] “Blockchain”.
- [11] “Blockchain Bandwagon Lesson”. *dinbits*. 2015.
- [12] “Why the Bitcoin Blockchain Beats Out Competitors”. *American Banker*. 2015.
- [13] Greenspan, Gideon. “Ending the bitcoin vs blockchain debate”.
- [14] “Secrets of Consistent Hashchains I: Eventual Consistency”. *Engineering DAPPs*. Retrieved 2015-11-02.
- [15] Aaron van Wirdum. “Student Aims to Boost Free Speech with Bitcoin Messaging App”.
- [16] Ken Shirriff. “Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software”.
- [17] “Bitcoin Strings: blockchain in words”
- [18] “CryptoGraffiti”.
- [19] Daniel Cawrey. “Why New Forms of Spam Could Bloat Bitcoin’s Block Chain”.
- [20] “What are the key differences between different ways of embedding messages in the blockchain?”.
- [21] Danny Bradbury. “Bitcoin, schmitcoin. Let’s play piggyback on the blockchain”.
- [22] “What is proof of existence?”.
- [23] Danny Bradbury. “Developers Battle Over Bitcoin Block Chain”.
- [24] Adam Black, Matt Corallo, Luke Dashjr, Mark Friedenback, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timon, and Pieter Wuille (2014). “An explanation of Bitcoin Sidechains”. Retrieved 22 October 2014.
- [25] SAMBURAJ DAS (2015). “The First SideChain for Bitcoin Exchanges”. *CryptoCoinsNews*.
- [26] “Why Bitcoin may herald a new era in finance”. *www.economistinsights.com*. The Economist Group. Retrieved 9 June 2015.
- [27] “Primavera De Filippi: From competition to cooperation”. *TEDxCambridge*. Retrieved 8 October 2015.

6.2 Cryptocurrency tumbler

A **cryptocurrency tumbler** or **cryptocurrency mixing service**^[1] is a service offered to mix potentially identifiable or ‘tainted’^[2] cryptocurrency funds with others, with the intention of confusing the trail back to the fund’s original source. Tumblers have arisen to improve the anonymity of popular cryptocurrencies, usually bitcoin, since they provide a public ledger of all transactions.^{[3][4]}

In traditional financial systems, the equivalent would be moving funds through banks located in countries with strict bank-secrecy laws, such as the Cayman Islands, the Bahamas and Panama offshore banks.

Tumblers take a small percentage **transaction fee** of the total coins mixed to turn a profit, typically 1-3%.^[5]

Mixing helps protect privacy, but can also be used for money laundering by mixing illegally obtained funds. Mixing large amounts of money may be illegal, being in violation of anti-structuring laws. **Financial crimes** author Jeffrey Robinson has suggested tumblers should be criminalized due their potential use in illegal activities, specifically funding terrorism,^[5] however a report from the **CTC** suggests such use in terrorism related activities is ‘relatively limited’.^[6]

There has been at least one incident where an exchange has blacklisted “tainted” deposits descending from stolen bitcoins.^{[7][8]} Manual or lightly automated mixing methods can make detection of taint more difficult unless the exchange follows the trail,^[9] but this approach does protect privacy like a true mixing service would.

The existence of tumblers has made the anonymous use of darknet markets easier and that of law enforcement harder.^[10]

6.2.1 Alternative implementations

Newer and proposed coin implementations such as Dash - (formally Darkcoin), Zerocoin^[11] and Cloakcoin have built in the mixing services as a part of their blockchain network.

The Dark Wallet client software for bitcoin was built to natively mix transactions between users to achieve the same effect without relying on a centralised service.^[12]

6.2.2 References

- [1] Jeffries, Adrienne (19 December 2013). "How to steal Bitcoin in three easy steps". Retrieved 17 May 2015.
- [2] Schweife, Dr. Johannes. "The taint and the Bitcoin". Retrieved 17 May 2015.
- [3] Bentley, Guy (12 May 2014). "Darkcoin: The cryptocurrency putting privacy first". Retrieved 17 May 2015.
- [4] "AN ANALYSIS OF ANONYMITY IN THE BITCOIN SYSTEM". Retrieved 28 May 2015.
- [5] Allison, Ian (February 11, 2015). "Bitcoin tumbler: The business of covering tracks in the world of cryptocurrency laundering". Retrieved 17 May 2015.
- [6] Brantly, Aaron (31 October 2014). "Financing Terror Bit by Bit". Retrieved 17 May 2015.
- [7] Buterin, Vitalik (21 May 2012). "MtGox: What the largest exchange is doing about the Linode theft and the implications". Retrieved 17 May 2015.
- [8] Mt Gox thinks it's the Fed. Freezes acc based on "tainted" coins.
- [9] Blockchain-based betting services function as mixing services?
- [10] IHS Jane's Intelligence Review (30 December 2014). "Law enforcement struggles to control darknet". Retrieved 6 July 2015.
- [11] Greenberg, Andy (13 January 2014). "Bitcoin Anonymity Upgrade Zerocoin To Become An Independent Cryptocurrency". Retrieved 17 May 2015.
- [12] Copestake, Jen (19 September 2014). "Hiding currency in the Dark Wallet". Retrieved 17 May 2015.

6.3 Proof-of-stake

Proof-of-stake is a method by which a cryptocurrency blockchain network aims to achieve distributed consensus. While the proof-of-work method asks users to repeatedly run hashing algorithms to validate electronic transactions,^[1] proof-of-stake asks users to prove ownership of a certain amount of currency (their "stake" in the currency). Peercoin^[2] was the first cryptocurrency to launch using Proof-of-Stake. Other prominent implementations are found in BitShares, Nxt, BlackCoin, NuShares/NuBits and Qora.

6.3.1 Block Selection Variants

Proof-of-stake must have a way of defining the next valid block in any blockchain. Selection by account balance would result in (undesirable) centralization, as the single richest member would have a permanent advantage. Instead, several different methods of selection have been devised.

Randomized Block Selection

Nxt and BlackCoin use randomization to predict the following generator, by using a formula that looks for the lowest hash value in combination with the size of the stake.^{[3][4][5]} Since the stakes are public, each node can predict - with reasonable accuracy - which account will next win the right to forge a block.

Coin Age Based Selection

Peercoin's proof-of-stake system combines randomization with the concept of “coin age,” a number derived from the product of the number of coins times the number of days the coins have been held. Coins that have been unspent for at least 30 days begin competing for the next block. Older and larger sets of coins have a greater probability of signing the next block. However, once a stake of coins has been used to sign a block, they must start over with zero “coin age” and thus wait at least 30 more days before signing another block. Also, the probability of finding the next block reaches a maximum after 90 days in order to prevent very old or very large collections of stakes from dominating the blockchain.^{[2][6][7]} This process secures the network and gradually produces new coins over time without consuming significant computational power.^[8] Peercoin's developer claims that this makes a malicious attack on the network more difficult due to the lack of a need for centralized mining pools and the fact that purchasing more than half of the coins is likely more costly than acquiring 51% of proof-of-work hashing power.^[9]

Velocity Based Selection

Reddcoin's 'Proof of Stake Velocity' (PoSV)^[10] claims to encourage velocity i.e. movement of money between people, rather than hoarding.

Voting Based Selection

Instead of only using the stake size, the block generators can be selected by votes. BitShares uses a system where stake is used to elect a total of 101 delegates, who are then ordered at random.^[11] This has many of the advantages of shareholder voting (for example, the flexible accountability enhance the incentives of the generators to act responsibly), and yet it reintroduces the dangerous sybil attack - as in one case where one user posed as the top five delegates.^[12]

6.3.2 Advantages

Proof of Work relies on energy use. According to a bitcoin mining-farm operator, energy consumption totaled 240kWh per bitcoin in 2014 (the equivalent of 16 gallons of gas).^[13] Moreover, these energy costs are almost always paid in non-cryptocurrency, introducing constant downward pressure on the price. Proof of Stake currencies can be several thousand times more cost effective.^[14]

The incentives of the block-generator are also different. Under Proof-of-Work, the generator may potentially own none of the currency he is mining. The incentive of the miner is only to maximize his own profits. It is unclear whether this disparity lowers or raises security risks.^[15] In Proof-of-Stake, those “guarding” the coins are always those who own the coins (although several cryptocurrencies do allow or enforce lending the staking power to other nodes).

6.3.3 Criticism

Some authors^{[16][17]} argue that proof-of-stake is not an ideal option for a distributed consensus protocol. One problem is usually called the “nothing at stake” problem, where (in the case of a consensus failure) block-generators have nothing to lose by voting for multiple blockchain-histories, which prevents the consensus from ever resolving. Because there is little cost in working on several chains (unlike in proof-of-work systems), anyone can abuse this problem to attempt to double-spend (in case of blockchain reorganization) “for free”.^[18]

Many have attempted to solve these problems:

- Peercoin uses centrally broadcast checkpoints (signed under the developer's private key). No blockchain reorganization is allowed deeper than the last known checkpoints. The tradeoff is that the developer is the central authority controlling the blockchain.
- Nxt's protocol only allows to reorganize last 720 blocks.^[19] However, this only rescales the problem: a client may follow a fork of 721 blocks, regardless of whether it is the tallest blockchain, preventing consensus.

- Ethereum's suggested Slasher protocol allows users to “punish” the cheater, who mines on the top of more than one blockchain branch.^[20] This proposal assumes you must double-sign to create a fork and that you can be punished if you create a fork while not having stake.

Statistical simulations have shown that simultaneous forging on several chains is possible, even profitable. But Proof of Stake advocates believe most described attack scenarios are impossible or so unpredictable that they are only theoretical.^{[21][22]}

6.3.4 See also

- Proof of Work
- Bitcoin
- Nxt
- Peercoin
- BlackCoin

6.3.5 References

- [1] Proof-of-Work vs Proof-of-Stake, 31-8-2014
- [2] King, Sunny. “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake” (PDF). Retrieved 2014-11-17.
- [3] “Nxt Whitepaper (Blocks)”. *nxtwiki*. Retrieved 2 January 2015.
- [4] mthcl (pseudonymous). “The math of Nxt forging” (PDF). *pdf on docdroid.net*. Retrieved 22 December 2014.
- [5] Vasin, Pavel. “BlackCoin’s Proof-of-Stake Protocol v2” (PDF).
- [6] Buterin, Vitalik. “What Proof of Stake Is And Why It Matters”. Bitcoin Magazine. Retrieved 2013-11-20.
- [7] Bradbury, Danny. “Third largest cryptocurrency peercoin moves into spotlight with Vault of Satoshi deal”. CoinDesk. Retrieved 2013-11-20.
- [8] Thompson, Jeffrey (15 December 2013). “The Rise of Bitcoins, Altcoins—Future of Digital Currency”. *The Epoch Times*. Retrieved 29 December 2013.
- [9] Whelan, Karl (2013-11-20). “So What’s So Special About Bitcoin?”. *Forbes*.
- [10] Ren, Larry. “Proof of Stake Velocity: Building the Social Currency of the Digital Age” (PDF).
- [11] “BitShares - Delegated Proof of Stake”. *bitshares.org*. Retrieved 2 January 2015.
- [12] “BitShares Sybil Attack Discussion”. *bitsharestalk.org*. Retrieved 2 January 2015.
- [13] “Carbon Footprint of Bitcoin”. *coindesk.com*. Retrieved 2 January 2015.
- [14] “Nxt Network Energy and Cost Efficiency Analysis” (PDF). Retrieved 21 December 2014.
- [15] “Proof of Work, Proof of Stake and the Consensus Debate”. *cointelegraph.com*. Retrieved 3 January 2015.
- [16] Andrew Poelstra. “Distributed Consensus from Proof of Stake is Impossible” (PDF).
- [17] Vitalik Buterin. “On Stake”.
- [18] “Hard Problems of Cryptocurrencies”.
- [19] “Nxt Whitepaper: History Attack”. *Nxtwiki*. Retrieved 2 January 2015.
- [20] Buterin, Vitalik. “Slasher: A Punitive Proof-of-Stake Algorithm”.
- [21] Chepurnoy, Alexander. “PoS forging algorithms: multi-strategy forging and related security issues” (PDF). *github.com*. Retrieved 30 December 2014.
- [22] Chepurnoy, Alexander. “PoS forging algorithms: formal approach and multibranch forging”. *scribd.com*. Retrieved 22 December 2014.

6.4 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.

6.4.1 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:[^]

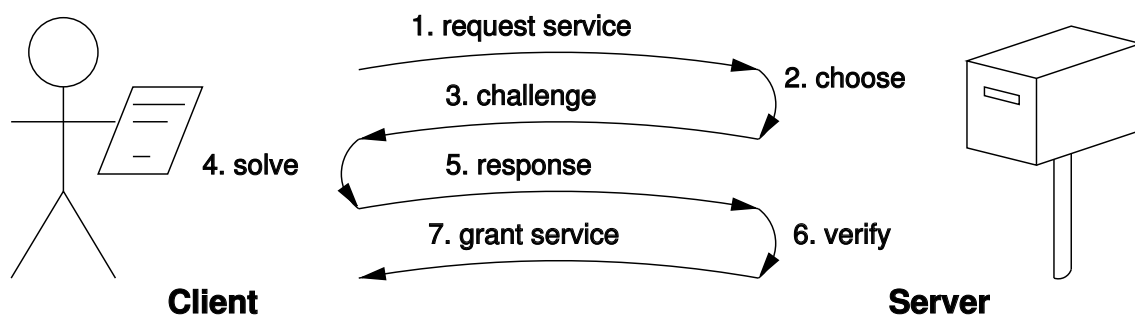
```
00000000000000756af69e2ffbdb930261873cd71
```

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.

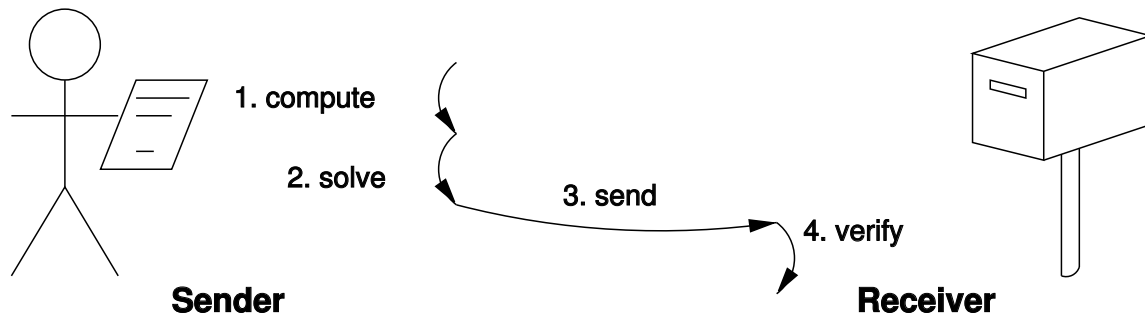
6.4.2 Variants

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.

6.4.3 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^{[1][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]

6.4.4 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.

6.4.5 Notes

1.^ On most Unix systems this can be verified with a command: `echo -n 1:52:380119:calvin@comics.net:::9B760005E92F0DAE | openssl sha1`

6.4.6 See also

- Bitcoin
- Cryptocurrency
- Bitmessage
- Proof-of-stake

6.4.7 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”. *Cryptography 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”. *Cryptography ePrint Archive, Report*.
- [18] “Reusable Proofs of Work”. Archived from the original on December 22, 2007.

6.4.8 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.*

6.5 Zerocoin

Zerocoin is a cryptocurrency proposed by Johns Hopkins University professor Matthew D. Green and graduate students Ian Miers and Christina Garman as an extension to the bitcoin protocol that would add true cryptographic anonymity to bitcoin transactions. Zerocoin was first implemented into a fully functional cryptocurrency by Gary Le and Poramin Insom, as the Moneta cryptocurrency. ^[1] Zerocoin provides anonymity by the introduction of a separate mixing service known as *zerocoin* that is stored in the bitcoin block chain. Though originally proposed for use with the bitcoin network, zerocoin could be integrated into any cryptocurrency.

6.5.1 Rationale

Bitcoin transactions are all stored, by design, in a public ledger (the **block chain**) that is accessible to everyone. These transactions provide privacy through **pseudonymity**, in that while each transaction is associated with the public address of the sender and receiver, the names of the owners of these addresses are at no time made known to the bitcoin network. To increase privacy, each person could create as many public addresses as they like, making it difficult to link transactions to the same person. If additional privacy were required, it is possible to **launder** bitcoin through a trusted third party, where the input coins are mixed in a large pool and output to a new address.^[2]

Regardless of the best precautions, by data mining of the block chain, it becomes possible in certain cases to link a set of public addresses to a specific (unnamed) individual. For example, this could be done by the analysis of spending habits, or by having the change of a transaction from one public address being sent to another. Furthermore, by utilizing information external to the block chain, such as public bitcoin addresses posted on a web site, or the postal address used with a bitcoin purchase, the possibility exists that every single bitcoin transaction of a given person could be determined.

Zerocoins are purchased with bitcoin in fixed denominations by a zerocoin mint transaction. Later, these zerocoins can be redeemed for bitcoin to a different bitcoin address by a zerocoin spend transaction. Through the use of **cryptographic accumulators** and **digital commitments** with **zero-knowledge proofs**, it is not possible to link the bitcoin address that was used to mint the original zerocoin to the bitcoin address used to redeem the zerocoin.

6.5.2 Zerocoin protocol

The zerocoin^[3] extension to bitcoin would have functioned like a money laundering pool, temporarily pooling bitcoins together in exchange for a temporary currency called zerocoins. While the laundering pool is an established concept already utilized by several currency laundering services, zerocoin would have implemented this at the protocol level, eliminating any reliance on trusted third parties. It anonymizes the exchanges to and from the pool using cryptographic principles, and as a proposed extension to the bitcoin protocol, it would have recorded the transactions within bitcoin's existing block chain.

The anonymity afforded by zerocoin is the result of cryptographic operations involved with separate zerocoin mint and spend transactions.^[3] To mint a zerocoin, a person generates a random serial number S , and encrypts (that is **commits**) this into a coin C by use of second random number r . In practice, C is a **Pedersen Commitment**. The coin C is added to a cryptographic accumulator by miners, and at the same time, the amount of bitcoin equal in value to the denomination of the zerocoin is added to a zerocoin escrow pool.

To redeem the zerocoin into bitcoin (preferably to a new public address) the owner of the coin needs to prove two things by way of a **zero-knowledge proof**. (A zero-knowledge proof is a method by which one party can prove to another that a given statement is true, without conveying any additional information apart from the fact that the statement is indeed true.) The first is that they know a coin C that belongs to the set of all other minted zerocoins (C_1, C_2, \dots, C_n), without revealing which coin it is. In practice, this is done quickly by use of a one-way **accumulator** that does not reveal the members of the set. The second is that the person knows a number r , that along with the serial number S corresponds to a zerocoin. The proof and serial number S are posted as a zerocoin spend transaction, where miners verify the proof and that the serial number S has not been spent previously. After verification, the transaction is posted to the blockchain, and the amount of bitcoin equal to the zerocoin denomination is transferred from the zerocoin escrow pool. Anonymity in the transaction is assured because the minted coin C is not linked to the serial number S used to redeem the coin.

The **accumulator** used for the zero-knowledge proof would have to be re-computed every time a spend transaction is verified, and although this can be done incrementally if the accumulator checkpoint is carried on from earlier blocks to the new block, it would still add some overhead to the verification-process. Additionally, both the accumulator checkpoint and all the zerocoin serial numbers would have to be added to every bitcoin block, thus increasing the size (although not substantially).

Since the verification process for zerocoins is much more computationally heavy than for bitcoins, the verification time for a block would increase up to 6 times depending on the ratio between bitcoins and zerocoins. Preliminary tests done by the developers show that even with the increased verification time and blocks twice the size of current bitcoin blocks, the verification time for an entire block would not exceed five minutes, and since a new bitcoin block is currently created every ten minutes on average, the increased verification time should not be a problem.^[3]

6.5.3 Moneta

Zerocoin was implemented into a fully functional cryptocurrency called Moneta. The Zerocoin software was first released to the public on December 18th, 2015^[1]

6.5.4 Criticism

One criticism of zerocoin is the added computation time required by the process, which would need to have been performed primarily by bitcoin miners. If the proofs were posted to the block chain, this would also dramatically increase the size of the block chain. Nevertheless, as stated by the original author, the proofs could be stored outside of the blockchain.^[4] To counter criticisms that the anonymity offered by zerocoin would facilitate illegal activity, it has been suggested that a *backdoor*, or other features, could be added to the zerocoin protocol to allow police to track money laundering, but this was not advocated in the original paper.^[5]

Since a zerocoin will have the same denomination as the bitcoin used to mint the zerocoin, anonymity would be compromised if no other zerocoins (or few zerocoins) with the same denomination are currently minted but unspent. A potential solution to this problem would be to only allow zerocoins of specific set denominations, however this would increase the needed computation time since multiple zerocoins could be needed for one transaction.

Depending on the specific implementation, the zerocoin protocol would rely on one or more trusted parties to generate two large prime numbers, p and q , so $n = p q$. Since n has to be hard to factor, p and q must be unknown to normal users for zerocoin to be secure. The protocol could rely on RSA unfactorable objects to avoid having to have a trusted party for the setup process.^[3] Such a setup, however, is not possible with the new Zerocash protocol.

6.5.5 Zerocash

The improved version of the protocol “that reduces proof sizes by 98% and allows for direct anonymous payments that hide payment amount” was announced on 16 November 2013.^[6] The developers presented their technical paper at the 2014 IEEE Security & Privacy Symposium along with launching the site.^[7]

The new protocol was called Zerocash. It is now not an extension to the bitcoin, but rather an independent technology with the same basic principles as blockchain and transactions, which was planned to implement in alt-coin.^[8] Zerocash utilizes succinct non-interactive zero-knowledge arguments of knowledge (also known as zk-SNARKs), a special kind of *zero-knowledge* method for proving the integrity of computations.^[9] Such proofs are less than 300 bytes long and can be verified in only a few milliseconds. However, zk-SNARKs require a large initial database for verifying (about 1.2 GB) and long time for producing a proof (spending the coin): 87 seconds to 178 seconds.^[10]

Between 5 October, 2015 and 11 January, 2016, the Zerocash website starting noting that “The Zerocash protocol is being developed into a full-fledged digital currency, Zcash.”^[11]

6.5.6 Bear Bonds

A faster implementation of zero knowledge proofs using zk-SNARKs was created for a new cryptocurrency called Bear Bonds. Bear Bonds requires only about 3 seconds and 85 KB of memory to create a transaction proof.^[12] Similar to Zerocash, Bear Bonds is an alt-coin with its own blockchain and transaction protocol.

6.5.7 References

- [1] Johnson, Amanda (18 December 2015). “First Implementation of Zerocoin Released: Introducing Moneta”. *Bitcoin News* (Bitcoin.com). Retrieved 18 December 2015.
- [2] Bradbury, Danny (7 June 2013). “How anonymous is Bitcoin?”. *CoinDesk* (CoinDesk Ltd.). Retrieved 8 February 2014.
- [3] Miers, Ian; Garman, Christina; Green, Matthew; Rubin, Aviel D. (May 2013). *Zerocoin: Anonymous Distributed E-Cash from Bitcoin* (PDF). 2013 IEEE Symposium on Security and Privacy. IEEE Computer Society Conference Publishing Services. pp. 397â€“411. doi:10.1109/SP.2013.34. ISSN 1081-6011.
- [4] Peck, Morgan E. (24 October 2013). “Whoâ€™s who in Bitcoin: Zerocoin hero Matthew Green”. *IEEE Spectrum* (Institute of Electrical and Electronics Engineers). ISSN 0018-9235. Retrieved 31 January 2014.

- [5] Hodson, Hal (13 March 2013). “Bitcoin add-on makes your virtual purchases private”. *NewScientist* (Reed Business Information Ltd.). ISSN 0262-4079. Retrieved 8 February 2014.
- [6] Matthew D. Green [matthew_d_green] (November 16, 2013). “We designed a new version of Zerocoin that reduces proof sizes by 98% and allows for direct anonymous payments that hide payment amount.” (Tweet). Retrieved September 16, 2015.
- [7] “Zerocash Main Page”.
- [8] “Matthew Green’s twitter”.
- [9] Ben-Sasson, Eli; Chiesa, Alessandro; Tromer, Eran; Virza, Madars (2014). “Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture”. *USENIX Security*.
- [10] “The verbatim record of M.Green’s talk at Real World Cryptography Workshop”.
- [11] <http://timetravel.mementoweb.org/list/20160111000000/http://zerocash-project.org/>
- [12] “Bear Bonds Whitepaper”.

6.5.8 External links

- Official website

Chapter 7

Text and image sources, contributors, and licenses

7.1 Text

- **Bitcoin Source:** <https://en.wikipedia.org/wiki/Bitcoin?oldid=700752533> *Contributors:* Damian Yerrick, Eloquence, Zundark, The Anome, Tommy-enwiki, Roybadami, Edward, Canton, Nealmcb, Michael Hardy, Fred Bauder, Liftarn, Ixfd64, Cyde, TakuyaMurata, DavidW-Brooks, Kingturtle, Julesd, Pratyeka, Glenn, CIPHERGO, Theamer, Mike Linksvayer, Susurrus, Samw, Ed Brey, Dcoetzee, Fuzheado, Andrewman327, WhisperToMe, TpbBradbury, Furrykef, Cleduc, Shizhao, Topbanana, Dbabbitt, AnonMoos, Drernie, Jni, Lambda, Nurg, Pjedicke, Rfc1394, Markewilliams, DataSurfer, Pifactorial, Tobias Bergemann, David Gerard, Psb777, Nelson Minar, Gil Dawson, Fudoreaper, HangingCurve, MSGJ, Marcica, 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, Pmsyzy, 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, 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, Veella, 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, Stalvert, Fleatham, 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, Spexxios, OpenToppedBus, Schandi, Mrschimpf, Alec.brady, Benlisquare, 020543m, Voodooom, Bgwhite, Manscher, Fcs, Aalegado, Wavelength, ThunderPeel2001, Conchisness, Mrienstra, Huw Powell, Cyferx, MJustice, Red Slash, Chosenken, Bhny, Piet Delpport, 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, SmartGuy Old, Yamaguchi, Gilliam, Portillo, Emj, Ohnoitsjamie, TrollDeBatalla, Sparge, Wcoenen, Chris the speller, Advorak, Thumperward, Elatanatari, GeraldKaszuba, V4vijayakumar, James Fryer, SvGeloven, Mdwh, Delink, Jerome Charles Potts, Jfsamper, Jdthood, Tekhnofiend, Kmag-enwiki, Ladislav Mecir, Lenin and McCarthy, Mike hayes, Fam-spear, Tamfang, Smallbones, Metallurgist, Frap, Zootreeves, Rrburke, Xyzyplugh, Kittybrewster, WhereAmI, Blue Matt, Fiskbullar, Ddas, Speedplane, WaldoJ, RolandR, BackDraft9387, Derek R Bullamore, Hgilbert, Nonstopdrivel, Sokolesq, Webjoe, Meni Rosenfeld, Piedmont, Springnuts, Juneblender, Byelf2007, Paul 012, Lambiam, Mike the k, Dmh-enwiki, Kaputa12, John, ZAB, Robofish, Plaiche, IronGargoyle, Nagle, Timothy, Melody Concerto, Makyen, DAVEMCARLSON, LARRYMCP, MECO, DR.K., ADJUSTABLEPLIERS, JEMORIN, DI2000, Jimisdead, Pjrm, Norm mit, DouglasCalvert, Kencf0618, Jmchugh, Clarityfiend, Courcelles, WakiMiko, TiriPon, Mikeyfaces, FatalError, Geremia, Jackzhp, Risoto2000-enwiki, Matthieu Houriet, Mgunn, JohnCD, Jokes Free4Me, N2e, Penbat, Thepm, Cydebot, Cahk, Danrok, Snarpel, Reywas92, Steel, Gogo Dodo, Jedonnelley, Maged123, Bposert, DumbBOT, Hontogaichiban, Biblbroks, Kozuch, Sckirklan, Arb, PamD, Ishdarian, Parsiferon, Davidhorman, EdJohnston, Gnrkel, Floridasand, Kjj31337, Izyt, Mmortal03, Utopiah, KrakatoaKatie, Ileresolu, CLSwiki, Seaphoto, Lovibond, Activist, Smartse, Mack2, Jdhowlett, Kmcnamee, 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, JL-Madrigal, Tekn04, Sipa1024, Logictheo, Mjbauer, Craig Mayhew, JaGa, TimidGuy, Gwern, Oren0, FisherQueen, Ekki01, Jimmilu, Rsrleigh, CommonsDelinker, Xiphosurus, ShoWPiece, Metallaxis, Trusilver, Maurice Carbonaro, Headinthedoor, Manderso, Smitemeister, Maproom, Toobaz, Lordgilman, 10mbt, Laytonsmith14, Tarinth, Leonarbe, NewEnglandYankee, Ontarioboy, Yablochko, Misbach, Tyraz, Ultra two, KylieTastic, Corriebertus, Ross Fraser, Ajfweb, Bonadea, Scott Illini, PdcCook, BernardZ, Loopback007, Davidr89, Cuzkatzimhut, VolkovBot, Thomas.W, Rubyuser, Fences and windows, Dom Kaos, Toddy1, QuackGuru, Redpointist, Philip Trueman, Giszmo-enwiki, Jogar2, Burpen, Sbjf, Chuckwolber, HannahKon, JUBALCAIN, Someguy1221, Cloudswrest, Jakebed, Rjm at sleepers, Noformation, Atheros1, UnitedStatesian, Unknownlight, Sheridan Zhoy, Ale85, Larklight, Agyle, Billinghurst, PeterEasthope, Cooperh, Celosia, Tigerchen, Ecnirpna99, 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, Sftg, S2000magician, HighInBC, Randomblue, MarkMLI, Tradedreddy, Mr. Stradivarius, Dabomb87, Denisarona, VanishedUser sdu9aya9fs787sads, ImageRemovalBot, Mr. Granger, Sfan00 IMG, Verbaetlittera, Ellassint, Keyur mithawala, SummerWithMorons, Jbening, Ethridgela, Dmurashchik, Blueyed, Cambrasa, KeithyIrwin, Quinxorin, Drmies, Der Golem, Frmorrisson, Leopard850, SuperHamster, Niceguyedc, Kamillas 1, Jswd, LeoFrank, Kitsunegami, Excirial, Socrates2008, Watchduck, Karlhendrikse, Sebleouf, NathanWalther, DrCroco, Arjayay, Tuchomator, Snacks, Tony Holkham, JasonAQuest, NintendoFan, Ecureuil espagnol, Chrisar-nesen, Zootboy, SF007, Lironah, M.grius, Twofivethreetwo, Jtjathomps, XLinkBot, Laser brain, Dthomsen8, Mitch Ames, Galzigler, Beach drifter, Mrcatzilla, MystBot, Glavkos, Dbrisinga, Addbot, Mckinley99, Mortense, Grayfell, FrankAndProust, Antonio92-enwiki, Thomasee73, AlbinoFerret, Mike30188, Mootros, TutterMouse, Franksensite, IceCreamEmpress, PhilosophyKing, Download, Laaknor-Bot, 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, Fragggle81, Louisstar, Legobot II, Ddcorkum, Amirobot, Sobich3ch, Denispir, Aoxfordca, R2D2!, Edoe, Rick Raubenheimer, Torsch, GamerPro64, Jerebin, Kirov Airship, Masharabinovich, Vroo, Dickdock, 4th-otaku, Dmarquard, DavidHarkness, AnomieBOT, Wikiyakapoola, DemocraticLuntz, John Holmes II, Message From Xenu, Jim1138, Interligator, Keithbob, L3lackEyedAngels, Mann jess, MaterialsScientist, 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, אוריאל, Riventree, Hobsonlane, Mu Mind, Quinn d, UncleNinja, Sanpitch, WikiDonn, Alarics, RoyGoldsmith, Timos m, Haeinous, Mfwitten, Kenfyre, Marcel van b, Redcert, Alex.ryazantsev, Greggydude, Weirdo10o4, Redrose64, Dusanson, Extramaster, OriumX, Gautier lebon, Pinethicket, Elockid, Alphazeta33, Lesath, Sander17, Intrepid-NY, Raphaelbastide, Calmer Waters, Smith98, The.megapode, Hisabness, Henriwatson, ContinueWithCaution, Cathy Richards, Rholme, Kylebk, Niri.M, Kgrad, Soundcomm, Thuckley89, Trappist the monk, Dchestnykh, Sirius-n, The Frenchie, Jesus Presley, Shellymoore3, Throwaway85, Lotje, Krassotkin, Callanec, Krisives, Athaba, Pommudivn, Miracle Pen, Bluefist, Mattmill30, Mcharnay, Aoidh, Cowlibob, David Hedlund, Jadair10, No One of Consequence, Vanzandij, Ivanvector, Fblan001, Chronulator, Skakkle, Stanjourdan, Suffusion of Yellow, EyeKnows, Skmacksler, Civic Cat, Jfmantis, JjusticeIV, Dree12, RjwilmsiBot, Sargdub, Ripchip Bot, VernoWhitney, Vivek.m1234, Phlegat, Mchcopl, Opticbit, HeinzzzderMann, Kiko4564, Rollins83, Steve03Mills, Rayman60, EmausBot, Cricobr, WikitanvirBot, Rathergood15, Observer6, Nuujinn, Philippe (WMF), Mjdtjm, Jibbsisme, Dewritech, GoingBatty, RA0808, Marco Guzman, Jr, Gogophergo, Antiquax, Qrsdogg, Torturella, NorthernKnightNo1, Your Lord and Master, Steve Lux, Jr., Mmeijeri, Wikipelli, Gagarine, Kaskaad, K6ka, Zeallous, Werieth, JD-DJS, Grondilu, ZéroBot, QuentinUK, John Cline, Checkingfax, Josve05a, Bollyjeff, Humanist09, Melksoft, Érico, Leotheleo, Mrmatiko, Jonpatterns, Fortheloveofbacon, Yiosie2356, 7partparadigm, Arpabone, L0ngpar1sh, Ocaasi, Casascius, Andre.Koster, Coubs514, JoeS-perrazza, Gonzo.Lubitsch, Libertaar, 0Core0, CJDuhaime, Palosirkka, Spobin, Gsarwa, Donner60, SBaker43, Do3cc-enwiki, Bulwersator, Ipsign, ChuispastonBot, Gandrewstone, AndyTheGrump, JanetteDoe, Targaryen, Jav wiki, Kai445, Ebehn, Doc Merlin, TitaniumCarbide, Davey2010, Voomoo, Cgt, Petr, Mikhail Ryazanov, ClueBot NG, HLachman, Johnnyshocker, George strawberry, Ullfund, Somedifferentstuff, Verpies, Ypnypn, LogX, Gilderien, Satellizer, Exposito, Polargeo 3, Tcatm, Magic 1million, Vacation9, Login-nigol, 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, Justinbassett, Roberticus, Dvtimes99, Esoteric10, FuFoFuEd, Astrohacker, Criticcon, WikiTryHardDieHard, The editor1900, Iselilja, Werowe, 13Goldem, Dpacmittal, Jcnetysys, Proudnewly1, Maccollie, Brustopher, TheN-Here, Batouzo, Neøn, ThisIsNotReal, JesseT77, Global Standard, MusikAnimal, Ecurrencies, Nikos 1993, Bitcoineer, Capivertx, GKFx, Sharpseek, Elucches, WinampLlama, Mark Arsten, Vermillion trade, Miraje182, Fbarousse, BitcoinTomWilliams, Socialmaven1, Exercisephys, Falkirks, Dmoores55, Juggernauts10, ChrisPDX, Izmailov, Mascarpouette, FormerNukeSubmariner, Terry4forex, Ainderby-quernhow, Ivan.a.tikhonov, Peterowenwilson, Majorbolz, Crh23, Bob Re-born, TheMacMini09, U4ealongan, Lxndr, MrBill3, GoCubs88, Rivoton, Victorsharpe, Tesssla, Cliff 12345, Thegreatgrabber, Kilidiplomus, TheGoodBadWorst, Steve.alleny, Rutebega, Cleanelephant, Clearish, Winston Chuen-Shih Yang, Samwalton9, MeanMotherJr, BattyBot, Factsearch, Sonba, Tkbx, Tutelary, Mleeds12, Riley Huntley, Testem, Zhaofeng Li, Kabesang Tales, JayBeeCool, Swetg, Phelix77, 0x0F, ChrisGualtieri, Larmsterpoet, JimNelin, CrunchySkies, Iolaka91823972, Electricmuffin11, Polarandwet, 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, Non-nompow, Lugia2453, Hto9950, Leptus Froggi, Frosty, Osyed1, Statecraft, HowardStrong, ComfyKem, Andyhowlett, 123sage321, Ez-zayakoo, SPECIFICO, Wik1p3d1a26, Danny Sprinkle, Gowthamkare, Telfordbuck, Leijurv, Another John S, Mariagvozd, Burrrito-Bazooka, Gatenosix, BeachComber1972, Anonymous68th, PinkAmpersand, Sr.ganador, Epicgenius, SolarStarSpire, Tsgeesq, BitBus, Hotelmason241, Ianpurton, Ruby Murray, Play Money for Dummies, Tomato expert1, Neoconfederate, EricLarson80, Mbmexpress, Kap 7, Surfer43, Dairhead, TinkleBear, Alf32, Wuerzele, Tango303, Dvdlevy120, JacquelineDerrida, Thkie, Flat Out, Byung do jung, New worl, Sarath divakar, Suumitgeek, KyleLandas, Akh81, Ndeine, NorthBySouthBaranof, FischTank, 51coin, Patrick2409, NottNott, MisterHungry, JoshDieter, Someone not using his real name, JeanLucMargot, Keepinternetfree, Jianhui67, Archlinux, TCMemoire, Oumot, MrScorch6200, DarkestElephant, DPRoberts534, XTC99LLC, Bojo1498, CameraWallet, Pinetreecrush, LaFayettePolitico, Lemonsdrops, Crow, JaconaFrere, G S Palmer, Lakun.patra, Marc Bago, Eliteware, JexsterB312, Tunacano, Unicodesnowman, ExtremeHeat11, CogitoErgoSum14, Vcwatcher, Mikhat, Encrypto1, Yoshi24517, Nyashinski, Jaumenez, YubbaDoo, Craigrotman, Currency cobano, Mattpalen, Silbtsc, Mojargon, BitcoinWiki, Hypnopompus, XDexus, Pigpie45, Bitbain, Krautski, Wiki man 195, Concord hioz, Monkbot, BarnstarFactory, BerkeleyLaw1979, JorgeGabriel, Powerful Lomax, Teaksmitty, Litecoinguy, Kitsios.a, J.vayner, SantiLak, OKNoah, Seppelpeters, Abckhxcvryu, Zulfikar ramzan, Wikifanman33, Dsprc, TitmanTrolled, BkDJk, Blue oracl2495, Manishvyas1747, Rextesexq, QuantOfAsia, Ali78v, Bobby223322, Shotsmc, Hats2543, Shadowzdx, ChrNPAL, Qwertym77, Mollyjohn1436, BitcoinrealityCheck, TwoEscarf, 12uihy, PirdPirdPrid, Milidepe, LampWithALeaf, WwATuu, Urunak, MARIODOESBREAKFAST, FOXIBOX, LoseKabel, Hannasnow, Robert-Rhys, Henryb2000, 10pippe, Bitslots, ChocTinFoil, LeeParq, Chunchi8, Hitechcomputeergeek, Vilalna, Titfditroyl, Superdavywavy, Eliteness, SpiltOctacle, MonteDaCunca, Unframboise, Thegrubbsian, Vinnie james, DissidentAggressor, Rooley555, Immanuel Thoughtmaker, EineCanardNoire, Myfare, HMSLavender, Ozzke, BitMeistern, Julia Eremina, Anotherusername1, Coin Collecting John, Zowayix001, Vvm3nelson, Homni, Wasill37, HamishPassion, Mozzzus, Akemaschite, Mario Castelan Castro, Caliburn, Phrackage, TheMagikCow, Kshanti07, ChamithN, Expresscoin, Bastian crypto, Webdesignersnow, AydinC, Tmarie3753, Jack Matelot, Jsthack, BITPUMP, Mtahaalam, BondNewYork, Adeyaya, Sysuwxm, Sealyy, TBroe, Primealgorith, Creationlayer, Liance, ThePenultimateOne, Brianrisk, Tenaqzn'f Fbyyqrq Gubat, Wuerzele2, E3b0c, Donate Bitcoin, Rog31905, TheCof-

feeAddict, YossiBoroPark, Esquivalence, Weegeerunner, Buchanjim, Mariksel, 4455tyui, Lothlorien317, BitTony, BoA-BTCopsec-14, TyHeers, Craftdraw, SoSivr, GimmeOpenRoad, Nysrtup, Acruxlit, THE GREY LINER, Kraainem, SaffronBacchus, BashCo, DiogoCao, Jimmylone, SpiryGolden, Ster3oPro, MariaAnnaWien, Zahirfahmi, I enjoy sandwiches, MLODROB, KasparBot, Ceannlann gorm, Samalter, Rickshawcraw, Pharaoh237, BitcoinX, LJWiki2000, Brollymook, 666AngelOfDeath, DylanMcKaneWiki, 𐄂, Conetry, Milko Zec, Wywyit, Pendletonian, VirtuOZ, Cashregister225, Malibubarbie, PeterVanDerStraaten, NorwayStorm, Gaelan, Furious Mythical Beast, D4m13nb3rry, FiddleFudger, Chevvin, PetitMonsieur, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Dr Lotus Black, Sfty, Cockblower, Brandonb01, AdmiredSneeze, 1FVLiNNTM65cxZ1rErevtEBLGHxzDMnVRY, Bitcoin Guy, Weltentstuermer, Qzd, Scott085, Ecoinseo, KryptoNatasha, 30has09, Mdclxvi0, Ghost of hugh glass and Anonymous: 943

- **Mastercoin** *Source:* <https://en.wikipedia.org/wiki/Mastercoin?oldid=690429044> *Contributors:* Topbanana, Benbest, Msgilligan, Slakr, Mmortal03, Vigyani, Agyle, Chrisarnesen, Softy, SporkBot, Martin Berka, Dexbot, Citation Needed, Mikhat, Nyashinski, NikosBentenitis, Panos Skourtis, Guttersville, MARIODOESBREAKFAST, Hannasnow, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 4
- **MazaCoin** *Source:* <https://en.wikipedia.org/wiki/MazaCoin?oldid=682224392> *Contributors:* Alexf, RHaworth, Codrinb, BiH, Cydebot, Magioladitis, Agyle, Georgemargaris, Excirial, Another Believer, AnomieBOT, FrescoBot, Jonpatterns, Davey2010, Parsley1972, Northamerica1000, BattyBot, Dexbot, Surfer43, Mandruss, Lewis Hulbert, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 6
- **Namecoin** *Source:* <https://en.wikipedia.org/wiki/Namecoin?oldid=687063232> *Contributors:* Anthony Fok, Bearcat, Matthäus Wander, Piotrus, Doc Taxon, Indolering, Oknazevad, Helohe, Lauciusa, MBisanz, Stesmo, Strait, Jwpii, RussBot, CambridgeBayWeather, MS-Japan, Deku-shrub, Eclipsed, RenegadeMinds, Amatulic, Snori, Ladislav Mecir, ElizaBarrington, DouglasCalvert, Medovina, DumbBOT, BrotherE, Magioladitis, Cat-five, CommonsDelinker, Smitte-Meister, Katharineamy, Jonytk, Agyle, Schulkin, Gnom, Nicholas Carraway, JL-Bot, Excirial, Another Believer, Chrisarnesen, Drpickem, Yobot, AnomieBOT, CoMePrAdZ, Breadblade, Yutsi, Spartin92, Dewritech, Your Lord and Master, Arpabone, ClueBot NG, Catlemur, BG19bot, Acoloss, Gronager, Dentalplanlisa, Cliff12345, Morning Sunshine, Domob, Riley Huntley, Phelix77, ChrisGualtieri, Tow, Dexbot, Rezonansowy, SoledadKabocho, Webclient101, Vintelok, HowardStrong, Sudoquai, JohnNBurke, François Robere, Neoconfederate, Surfer43, NorthBySouthBaranof, FDMS4, Someone not using his real name, TheJediMaster777, Kubrixcube, Tskweres, Saectar, Yoshi24517, St170e, Sequencer11, Filedelinkerbot, Vieque, Beth-Naught, MARIODOESBREAKFAST, Namecoin, Dwda, Jointed.owl, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 37
- **NuBits** *Source:* <https://en.wikipedia.org/wiki/NuBits?oldid=690428145> *Contributors:* Nick Number, CommonsDelinker, XLinkBot, Narutolovehinata5, Yobot, Adam9007 and Ttutdxh
- **Peercoin** *Source:* <https://en.wikipedia.org/wiki/Peercoin?oldid=688148084> *Contributors:* Andrewman327, Gracefool, Discospinster, Intersofia, Amatulic, Jerome Charles Potts, Medovina, Barek, Magioladitis, Mufka, Rdjere, Agyle, C0unterph0bia, Repat, EBY3221, Arjayay, Another Believer, Chrisarnesen, Hmockey, Nkot, Yobot, AnomieBOT, LilHelpa, Solphusion-enwiki, Hromi, Breadblade, Orenburg1, Fillipo23, Treer, I'm not human, VinceSamios, Fmably, WikiTryHardDieHard, Cliff12345, BattyBot, ChrisGualtieri, Dexbot, Rezonansowy, Mogism, Sotdan, PinkAmpersand, Epicgenius, SolarStarSpire, DavidLeighEllis, PostScarcity, Rayoncadet12, NorthBySouthBaranof, Financialknowledge, AnonymousWiking, Cereza123, WikiJuggernaut, JorisVR, Ppcoinwikipeercoin, Tskweres, Wikitodayh767, Cryptoenthusiest, WPCryptoCurrency, Cothanmiller, TheBagog, HoopJumper, Litecoinguy, Rabazos, V-apharmd, MARIODOESBREAKFAST, TheMagikCow, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, ZnS-N and Anonymous: 60
- **Titcoin** *Source:* <https://en.wikipedia.org/wiki/Titcoin?oldid=692250691> *Contributors:* Greenman, Bearcat, Joe Decker, Rosekelleher, Yobot, Hell in a Bucket, GoingBatty, Kbrzoznowski, Darylgolden, MARIODOESBREAKFAST, Iaritmioawp, Hapanyc, Takodah, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 3
- **Auroracoin** *Source:* <https://en.wikipedia.org/wiki/Auroracoin?oldid=700546071> *Contributors:* Greenman, Anthony Appleyard, Koavf, Pburka, Tony1, Aggie80, Aozuas, Agyle, Yngvadottir, ONaNele, Tristan 10o, GoingBatty, Mz7, BG19bot, Wi11337, Citation Needed, DavidLeighEllis, Stirling7, MARIODOESBREAKFAST, WinterstormRage, Charles-Edouard de la Pannerie de la Villardière de Mardricourt, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 16
- **Coinye** *Source:* <https://en.wikipedia.org/wiki/Coinye?oldid=687171300> *Contributors:* Auric, Ricky81682, Deku-shrub, Hgilbert, DumbBOT, Burt777, Agyle, Mortense, AnomieBOT, Danno uk, Quebec99, Breadblade, Tuankiet65, TcomptonMA, Smeirow, ClueBot NG, Djodjo666, Widr, BG19bot, Mark Arsten, BattyBot, Ntmbeast, Rezonansowy, WOLF LAMBERT, Citation Needed, Epicgenius, Xt0rt3r, Tedl4vender, Daret Masampullmor, DPRoberts534, Nyashinski, Nelsonmorrow, Taco Viva, Mangledblue, Delt84, Liance, SpiryGolden, Coindog08, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 25
- **Dogecoin** *Source:* <https://en.wikipedia.org/wiki/Dogecoin?oldid=699640434> *Contributors:* Canton, Greenman, Anders Feder, Julesd, Mxn, Samsara, Jeffq, David Gerard, Michael Devore, Thorwald, Discospinster, ArnoldReinhold, Dbachmann, Stesmo, Johnmarkos, Danski14, Atomicthumbs, Geraldshields11, Skyring, KTC, Daranz, Aerowolf, Tabletop, Ahazred8, Mendaliv, Nihiltres, Crazeman, King of Hearts, Benlisquare, DVdm, Cybercat, Mal7798, Josh3580, Dspradau, DesignExplosion, Prodego, Gilliam, Amatulic, Underbar dk, Ser Amantio di Nicolao, Jourdain, Espreon, Kencf0618, Fulvio, TXAggie, Cydebot, Gogo Dodo, Siberian Husky, Nekng, Guineapigs, Nick Number, Pnosker, Leuqarte, Ingolfson, Barek, CommonsDelinker, Eduemoni, Smitte-Meister, Ontarioboy, KylieTastic, Ajfweb, YKgm, JUBALCAIN, Wiae, Agyle, Skunky6969, Thehornet, Flyer22 Reborn, Jonahtrainer, Georgemargaris, Tradedreddy, ImageRemovalBot, SuperHamster, Excirial, Another Believer, Tezero, Ant59, XLinkBot, Mortense, Ironholds, Download, Fivexthethird, Yobot, Fraggle81, Shard013, Taneb, Samtar, Ayceman, AnomieBOT, Jim1138, Materials scientist, Jwiechers-enwiki, LilHelpa, Amaury, Phette23, I dream of horses, CraftyPirate, DimiFW, Jyp2000, Callanec, Darsie42, Kapooh, ErikvanB, TheMesquito, Mean as custard, JjusticeIV, Jw12321, Tuankiet65, Kaigenji, Arrakis3k, GoingBatty, Avdonin, Winner 42, Wikipelli, K6ka, Tdodds, Checkingfax, Josve05a, Cyan Ryan, Derekleungszhei, IamYoshi, Champbronc2, GeorgeBarnick, ClueBot NG, Satellizer, HongxuChen, Dennis97519, Sarik233, VinceSamios, Lawsonstu, Kevoras, Lowercase sigmabot, BG19bot, Mark Arsten, The Almighty Drill, Blaspie55, DotHectate, Samwalton9, BattyBot, Mdann52, ChrisGualtieri, ZappaOMati, Elieltavares, CrunchySkies, Azure94, Robin van der Vliet, Felixphew, Dexbot, Rezonansowy, Citation Needed, NFLisAwesome, JasonMacker, Pokajanje, Jodapop, Andyhowlett, TortoiseWrath, Bugzeeolboy, Ekips39, OwenVersteeg, SolarStarSpire, Tentinator, Everymorning, Soffredo, Xt0rt3r, Wuerzele, PettR, GreaseballNYC, ElHef, Marsroverr, Nihaofish, Ugog Nizdast, NorthBySouthBaranof, Cyclonelsaac, Quenhitran, DungeonSiegeAddict510, Marukaitechikyuu, Phoenix616, Konveyor Belt, Br100x, Julian888888888, SamanthaPuckettIndo, Mralex20, Second Skin, Ivan Kwong, Yoshi24517, Nyashinski, Slumdoge, Nekomata3, Mattpalen, Billym2k, Rswire, Cicecx, Vkozlovu, Filedelinkerbot, J4g!XFZjU, Elreiner, Js1234567, ApharionDeSol, MatthewBuchwalder, GXPurchases, Miamore101, Shimy249, Nmek, Aqrulesms, Lattepatrick, Batminem, Edmundluong,

N4djb0t, Faceyourfaces, Nosolutions, CoolStoryBro42, VespertilioX, Eglu81, BkDJk, Dogekingdotnet, Doyouevenban2, NonCamel-Case, Catoshi, MarkiPoli, Scroteskin, MARIODOESBREAKFAST, Erwinbantilan, Purpleshire, Onlyamuffin, Croteaumj, MaxLangley, Mistervise33, Zeklandia, Vinnie james, Dogerhymeswithvogue, Nutbun, Pwnerast, Pyds1977, Liance, Motleyshibe, Alleswurscht, The-limiter, Doge100, Addict4bitcoin, Pharoah237, Beardog108, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Johanvanl, Kozan Huseyin and Anonymous: 226

- **Litecoin** *Source:* <https://en.wikipedia.org/wiki/Litecoin?oldid=700046696> *Contributors:* Canton, Greenman, Lensi, Pigsonthewing, Ds13, Beland, Shiftchange, Pmsyzz, Stesmo, Lectorar, Katana, Zntrip, Dandv, Bgwhite, RussBot, Pburka, Deku-shrub, Luke-Jr, Ohnoitsjamie, Ladislav Mecir, Spikeman, Cherry, Kirbykirbykirby3, Cydebot, Reywas92, Medovina, DumbBOT, Dstruct2k, Barek, OhanaUnited, Magioladitis, CFCF, ST1V-enwiki, Rdjere, Jeff G., Agyle, Jimthing, Jonathrainer, Hatster301, Trivialist, Another Believer, Mortense, DElogics, Kuzetsa, Yobot, Fraggel81, Auronrenouille, AnomieBOT, Jim1138, Amaury, Txaggiemichael, FrescoBot, Breadblade, Pinethicket, Txt.file, Aoidh, Wschlitz, Mean as custard, EmausBot, Tuankiet65, Mjdtjm, Compgenius, Tanner Swett, Arpabone, Siowtuze, Gambit-Declined, Catlemur, Gilderien, Xcess96, O.Kosowski, VinceSamios, Newyorkadam, Lawsonstu, Strike Eagle, BG19bot, Socram8888, Aktivradio, Neon, Exercisephys, Karlyboy, Cliff12345, Samiunn, Tkbx, Razzintown, ChrisGualtieri, Rezonansowy, JPhebus, Statecraft, James12345, HowardStrong, Cornelismchl, ChocoboLee, Mo5ul, Jocoder5, François Robere, Dairhead, Coin12349, Rancor60, Aspect76, CryptoAddicto, Taktao, Ltcbtc, CryptoDefender, NorthBySouthBaranof, Ijflh, AnonymousWiking, Makkachin, TheJediMaster777, DPRoberts534, MarkTee, Thomasconn, Tskweres, Mayankasthana1993, Btcde, Nvk-original, Nihondino, Eliteware, FOJIK, Dr-crypto88, Hiberio, Pbnysen, Jamesmcgovern, Mikandjo, Nyashinski, Mattpalen, Rswire, Litecoinguy, MatthewBuchwalder, Rabazos, Fafasiu, Earthcosmos, Pietro barbiero, Guttersville, MARIODOESBREAKFAST, Hannasnow, Ozzke, Wasill37, Mozzzus, TheCoffeeAddict, Mark Biter, SpiryGolden, Samalter, Pharoah237, Wikihelpful, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Losh1212 and Anonymous: 160
- **PotCoin** *Source:* <https://en.wikipedia.org/wiki/PotCoin?oldid=689484332> *Contributors:* Nihiltres, Deku-shrub, Mild Bill Hiccup, Cuaxdon, Cnwiliams, Cwmhiraeth, BG19bot, MARIODOESBREAKFAST, Mrjonesmtl, Deemington, Liance, Chrismewhort, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, ElectricController, OriginalMrCoin and Anonymous: 3
- **CryptoNote** *Source:* <https://en.wikipedia.org/wiki/CryptoNote?oldid=695211901> *Contributors:* David Latapie, Piotrus, Stesmo, Cydebot, CommonsDelinker, Revent, Jerryobject, Arjayay, Yobot, AnomieBOT, Bollyjeff, BG19bot, BattyBot, Mogism, Lemnaminor, The Herald, Işta Devatā, MARIODOESBREAKFAST, Hannasnow, Devrilz, Terry Richardson, Amoebatron-enwiki, PeterCheng93, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 14
- **Monero (cryptocurrency)** *Source:* [https://en.wikipedia.org/wiki/Monero_\(cryptocurrency\)?oldid=697206507](https://en.wikipedia.org/wiki/Monero_(cryptocurrency)?oldid=697206507) *Contributors:* David Latapie, Stesmo, Yamaguchi, Ser Amantio di Nicolao, Mmortal03, Arjayay, Yobot, AnomieBOT, FrescoBot, BG19bot, Masum Ibn Musa, MARIODOESBREAKFAST, Hannasnow, Nemesis0618, Terry Richardson, Amoebatron-enwiki, Procrypto, RentaCat, Lleits, Nomorenono and Anonymous: 11
- **Dash (cryptocurrency)** *Source:* [https://en.wikipedia.org/wiki/Dash_\(cryptocurrency\)?oldid=685496789](https://en.wikipedia.org/wiki/Dash_(cryptocurrency)?oldid=685496789) *Contributors:* Jni, Bearcat, Cool Hand Luke, Piotrus, Zntrip, Ser Amantio di Nicolao, Mmortal03, Agyle, Terrorist96, Tassedethe, Yobot, AnomieBOT, Amaury, I dream of horses, BG19bot, Raze182, Aisteco, BattyBot, Cyberbot II, Citation Needed, Jodosma, Surfer43, DavidLeighEllis, JustBerry, Davidbentolila, Nzoomed, MARIODOESBREAKFAST, Hannasnow, Liance, Tesquenure, Pharoah237, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, 89sec and Anonymous: 19
- **Primecoin** *Source:* <https://en.wikipedia.org/wiki/Primecoin?oldid=682809351> *Contributors:* Michael Hardy, Scryer-enwiki, Postdlf, Brianhe, Hritcu, Giraffedata, RoySmith, Joe Decker, Benlisquare, Pburka, Roques, Jerome Charles Potts, Sadads, Frap, A5b, Intelliot, Slakr, Medovina, Mojo Hand, Maqayum, Magioladitis, Black Kite, Rdjere, Agyle, SuperHamster, Excirial, Another Believer, Mhockey, Yobot, AnomieBOT, Amaury, Hell in a Bucket, IlyaVak, Mt4928, Jonpatterns, Bardi1100, BG19bot, WikiTryHardDieHard, Cliff12345, Tutelary, Cyberbot I, Hassanisahba, Rezonansowy, Citation Needed, Epicgenius, SolarStarSpire, NorthBySouthBaranof, Matuhin86, AnonymousWiking, Swchong25, Eliteware, Impsswoon, WPCryptoCurrency, Kamnxt, Nyashinski, Batminem, Guttersville, MARIODOESBREAKFAST, Hannasnow, Pharoah237, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 27
- **Ethereum** *Source:* <https://en.wikipedia.org/wiki/Ethereum?oldid=700327392> *Contributors:* Greenrd, David Gerard, Khalid hassani, Beland, Piotrus, Shiftchange, Smyth, Pk2000, Woohookitty, Deeahbz, Deku-shrub, LarsPensjo-enwiki, Valoem, Bryan P. C. C., Mfortier, JonathanCross, Keith D, Leyo, Varnent, Agyle, Trustable, Niceguyedc, Trivialist, Download, Softy, Jerebin, AnomieBOT, LilHelpa, Sampire, Jonathandeamer, LittleWink, Jonesey95, Fossilet, Ruxkor, Jonpatterns, ClueBot NG, Gareth Griffith-Jones, Malefizer, BG19bot, BattyBot, Escalicha, Citation Needed, SolarStarSpire, RaphaelQS, DigitalImpostor, Cyphertribe, Cnas13, MARIODOESBREAKFAST, Hannasnow, AntipodeBomb, Warmoak, Poridge123, Elmeter, Aliensyntax, Drupalnomad, Alterneck, MaxKordek, Johanvanl, Fremtid and Anonymous: 43
- **BlackCoin** *Source:* <https://en.wikipedia.org/wiki/BlackCoin?oldid=656826141> *Contributors:* Greenman, Piotrus, JHCaufield, Adamkry, XLinkBot, Laser brain, Yobot, AnomieBOT, Northamerica1000, BattyBot, Citation Needed, FLOat1NGP01NT001, Hannasnow, Greenmon2, Creneo, WinterstormRage and Anonymous: 7
- **Counterparty (technology)** *Source:* [https://en.wikipedia.org/wiki/Counterparty_\(technology\)?oldid=681228232](https://en.wikipedia.org/wiki/Counterparty_(technology)?oldid=681228232) *Contributors:* Giraffedata, Bhny, Dialectric, Amatulic, Cydebot, Agyle, SchreiberBike, Yobot, Jonpatterns, Mathew105601, BG19bot, Northamerica1000, BattyBot, Citation Needed, UY Scuti, Coinburger, MARIODOESBREAKFAST, Notsoshifty, Moontreasure, PookTwo, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Johanvanl and Anonymous: 13
- **NEM (cryptocurrency)** *Source:* [https://en.wikipedia.org/wiki/NEM_\(cryptocurrency\)?oldid=696207135](https://en.wikipedia.org/wiki/NEM_(cryptocurrency)?oldid=696207135) *Contributors:* Pigsonthewing, ZimZalaBim, RussBot, Number 57, Jeff.t.mcdonald, Shawnleary, Cydebot, Michig, CommonsDelinker, CorenSearchBot, OgreBot, Jonpatterns, Unicodesnowman, Hannasnow, Jonathanarpith, D-5000, Loi.tranquang, Joseph2302, Nyanpi, Rockethead123, Mixmaster2, Makoto1337, Renolteng.li, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 7
- **Nxt** *Source:* <https://en.wikipedia.org/wiki/Nxt?oldid=691006219> *Contributors:* Topbanana, Bearcat, Thomas Veil, Piotrus, OneGuy, Bgwhite, RussBot, Deku-shrub, Sandstein, Cydebot, Kadmium, Leyo, Agyle, Unbuttered Parsnip, Yobot, AnomieBOT, Biljerk101, Breadblade, Emisanle, BG19bot, Cyberbot I, SJ Defender, Salsacz, Jjamesryan, Ironchapel, CryptoInvestor777, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, DamelonNxt, Rpmconsult and Anonymous: 8
- **Ripple (payment protocol)** *Source:* [https://en.wikipedia.org/wiki/Ripple_\(payment_protocol\)?oldid=687823136](https://en.wikipedia.org/wiki/Ripple_(payment_protocol)?oldid=687823136) *Contributors:* Taral, Michael Hardy, Dtgm, Areyu42, Altenmann, Beefman, Beland, DNewhall, Spoirier-enwiki, Lycurgus, VanGore, Stesmo, GrantNeufeld, Fasten, Bobrayner, MartinSpacek, Mindmatrix, Singpolyma, Toussaint, Koavf, Bgwhite, ColdFeet, RussBot, Robert Will, Dialectric, Nirvana2013, Noddycr, GraemeL, SmackBot, Chris the speller, Bluebot, Jerome Charles Potts, Piroroadkill, Fiskbullar, Rgrant, Derek

- R Bullamore, Bn, DO11.10, RomanSpa, Jackzhp, JohnCD, Penbat, Cydebot, DumbBOT, Thijs!bot, EdJohnston, L0b0t, Barek, Skomorokh, Magioladitis, Homunq, RomualdoGrillo, Robustus, Mårten Berglund, Jspiegler, Lunokhod, Touisiau, Bonadea, TouristPhilosopher, Agyle, Rougieux, Michael Frind, Simbamford, Rfugger, X-Fi6, Sfan00 IMG, Niceguyedc, Kitsunegami, Chrisarnesen, Miami33139, Addbot, Mortense, MrOllie, Yobot, Backfromquadrangle, 4th-otaku, AnomieBOT, Mbiama Assogo Roger, JimVC3, Jeune17, Ehir, Sanpitch, David290, Frank Mottley, John of Reading, GoingBatty, Ballofstring, Mmeijeri, Kaskaad, Captain Awesome Power, Ipsign, Catlemur, Ramaksoud2000, Emisanle, Jeraphine Gryphon, BG19bot, Hallows AG, Compfreak7, Cliff 12345, Ipetts, Cyberbot I, Cyberbot II, ChrisGualtieri, Earflaps, APerson, Rezonansowy, Citation Needed, Epandurski, Neoconfederate, Sayitclearly, Rahul Bott, Comp.arch, Xrptalk, Hyh123, Someone not using his real name, Mangostaniko, Rippleport, Unicodesnowman, Olenyash, PirateButtercup, Litecoinguy, Bitcoindarling, Guttersville, Xrptrader, Keepx, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 97
- **Stellar (payment network)** *Source:* [https://en.wikipedia.org/wiki/Stellar_\(payment_network\)?oldid=697214987](https://en.wikipedia.org/wiki/Stellar_(payment_network)?oldid=697214987) *Contributors:* DragonflySixtyseven, Tabletop, Amatulic, Gabriel Kielland, Sfan00 IMG, Mild Bill Hiccup, XLinkBot, Dthomsen8, Dawynn, Yobot, Jeune17, HongxuChen, Rinaku, Chisme, Be..anyone, BattyBot, Khv422, J. S. Gutenberg, Andrewfromstellar, CryptoPrincess, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 2
 - **Block chain (database)** *Source:* [https://en.wikipedia.org/wiki/Block_chain_\(database\)?oldid=699581273](https://en.wikipedia.org/wiki/Block_chain_(database)?oldid=699581273) *Contributors:* 5ko, DavidCary, Khalid hassani, Danhash, Clotho, Intgr, Sneak, Deku-shrub, Eclipsed, Ladislav Mecir, Aldaron, Jfayel, Philippschaumann, PamD, Mmortal03, Ontarioboy, Zxsmt, Trivialist, Rhododendrites, AnomieBOT, Jim1138, Trappist the monk, Eeik, Ivanvector, Jonpatterns, Casascius, BG19bot, Alloy020, Powerful Lomax, Vwm3nelson, Wikihelpful, Drupalnomad, Drjohncavazos, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Webnator, Rt665j4, Jpkabin, OnePercent, Abrrr5583, Singleissuevoter and Anonymous: 25
 - **Cryptocurrency tumbler** *Source:* https://en.wikipedia.org/wiki/Cryptocurrency_tumbler?oldid=694352321 *Contributors:* Deku-shrub, Mike1901, Jonpatterns, Jeraphine Gryphon, BG19bot, Hannasnow, Arthistorian1977, ₩₩, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR and Anonymous: 4
 - **Proof-of-stake** *Source:* <https://en.wikipedia.org/wiki/Proof-of-stake?oldid=695753237> *Contributors:* Greenman, Tobias Bergemann, Thomas Veil, Philosophistry, Uporo, Gilliam, Ladislav Mecir, Andrewhime, Fiskbullar, Geesu, Neil Smithline, X-Fi6, Unbuttered Parsnip, Arjayay, Jytdog, Mmfioire, Chilin, Wargo, AnomieBOT, Sanpitch, Breadblade, Mctaino, Jonpatterns, Jmreinhardt, BG19bot, Ofomenko, BattyBot, ArmorShieldA99, ChrisGualtieri, Jstollman323, TheJediMaster777, Saectar, Cypherious, Litecoinguy, AKS.9955, Weeks1956, Hannasnow, Ozzke, Greenmon2, PLear, KenCode, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Lleits, Nomorenono and Anonymous: 38
 - **Proof-of-work system** *Source:* https://en.wikipedia.org/wiki/Proof-of-work_system?oldid=697206261 *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, JustAGal, Davidhorman, SeanTater, Albany NY, Magioladitis, NoDepositNoReturn, Yakushima, Logictheo, David Eppstein, Gwern, Ontarioboy, TreasuryTag, Gizmo-enwiki, Nicksh, Mumiemonstret, SuzieDerkins, Chrisarnesen, Mehmud, Miami33139, XLinkBot, Addbot, AnomieBOT, DannyAsher, Omnipaedista, Breadblade, Jesse V., RjwilmsiBot, Joeyhewitt, Mmeijeri, Euloiox, Jonpatterns, H3llBot, L0ngpar1sh, Ipsign, 4368a, BG19bot, Cliff12345, 0x0F, Tuxayo, Wuchang, Adam2us, Play Money for Dummies, PostScarcity, Omninonsense, Saectar, Unicodesnowman, YubbaDoo, Monkbot, MARIODOESBREAKFAST, FOXIBOX, Hannasnow, Vivi239, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, JonBobbie and Anonymous: 58
 - **Zerocoin** *Source:* <https://en.wikipedia.org/wiki/Zerocoin?oldid=699295102> *Contributors:* Piotrus, BD2412, Bgwhite, Elatanatari, Frap, J. Finkelstein, JonathanCross, Barek, Magioladitis, Lunokhod, AKA MBG, Cloudswrest, Agyle, Int21h, Another Believer, Chrisarnesen, Yobot, Amaury, Sanpitch, Hell in a Bucket, David Hedlund, EmausBot, K6ka, Mz7, BG19bot, Jor.langneh, Hamish59, Cliff12345, 0x0F, APerson, Rezonansowy, Citation Needed, SolarStarSpire, Jodosma, Surfer43, DavidLeighEllis, Comp.arch, Slashdottir, TheDragonFire, Nyashinski, Litecoinguy, Dsprc, Hannasnow, Calhba, Kbrowser, Zerovert, Pharoah237, 1Wiki8Q5G7FviTHBac3dx8HhdNYwDVstR, Bbnov5, ArguMentor and Anonymous: 16

7.2 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:6_Full_Logo_S-2.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/2/24/6_Full_Logo_S-2.png *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Losh1212
- **File:Adding_Trust_and_Allowing_Rippling.jpg** *Source:* https://upload.wikimedia.org/wikipedia/en/4/4a/Adding_Trust_and_Allowing_Rippling.jpg *License:* Public domain *Contributors:* the open sourced client can be found at <https://github.com/ripple> *Original artist:* Ripple Labs
- **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:Ambox_wikify.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/e/e1/Ambox_wikify.svg *License:* Public domain *Contributors:* Own work *Original artist:* penubag
- **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_Transaction_Visual.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/cc/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_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:BlackFlagSymbol.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/9/95/BlackFlagSymbol.svg> *License:* CC BY 3.0 *Contributors:* Transferred from en.wikipedia to Commons. *Original artist:* The original uploader was Jsymmetry at English Wikipedia
- **File:Coinye.png** *Source:* <https://upload.wikimedia.org/wikipedia/en/4/4b/Coinye.png> *License:* Fair use *Contributors:* <http://coinyecoin.org/assets/coinye.png> *Original artist:* ?
- **File:Commons-logo.svg** *Source:* <https://upload.wikimedia.org/wikipedia/en/4/4a/Commons-logo.svg> *License:* ? *Contributors:* ? *Original artist:* ?
- **File:Counterparty.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/4/40/Counterparty.png> *License:* MIT *Contributors:* <https://github.com/CounterpartyXCP/counterparty-gui/blob/develop/assets/counterparty.png> *Original artist:* Present Counterparty Developers
- **File:Counterparty_xcp_symbol.png** *Source:* https://upload.wikimedia.org/wikipedia/en/1/17/Counterparty_xcp_symbol.png *License:* Fair use *Contributors:*
The logo is from the <http://counterparty.io> website. <http://counterparty.io/support/#logos> *Original artist:* ?
- **File:Counterwallet_Homepage.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/9e/Counterwallet_Homepage.png *License:* Copyrighted free use *Contributors:* <https://github.com/xnova/counterwallet> *Original artist:* Counterparty Team
- **File:CryptoNote_blockchain_analysis_ambiguity.gif** *Source:* https://upload.wikimedia.org/wikipedia/commons/6/6e/CryptoNote_blockchain_analysis_ambiguity.gif *License:* CC BY-SA 3.0 *Contributors:* <https://cryptonote.org/inside#untraceable-payments> *Original artist:* CryptoNote official site
- **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:Crystal_Clear_app_kedit.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/e/e8/Crystal_Clear_app_kedit.svg *License:* LGPL *Contributors:* Sabine MINICONI *Original artist:* Sabine MINICONI
- **File:DEVCON_0_group_photo.jpeg** *Source:* https://upload.wikimedia.org/wikipedia/commons/6/6f/DEVCON_0_group_photo.jpeg *License:* Attribution *Contributors:* <https://twitter.com/ethereumproject/status/538505582152806400> *Original artist:* Eth Dev Ltd.
- **File:DarkNote_wallet.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/e/e5/DarkNote_wallet.png *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* MARIODOESBREAKFAST
- **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:Difficulty.svg** *Source:* <https://upload.wikimedia.org/wikipedia/en/6/6d/Difficulty.svg> *License:* ? *Contributors:*
Own work
Original artist:
Ladislav (talk) (Uploads)
- **File:Dogecoin.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/b/b4/Dogecoin.png> *License:* MIT *Contributors:* <https://github.com/dogecoin/dogecoin/blob/master/src/qt/res/icons/bitcoin.png> *Original artist:* Dogecoin Developers
- **File:Dogecoin_Paper_Wallet.jpg** *Source:* https://upload.wikimedia.org/wikipedia/en/c/c1/Dogecoin_Paper_Wallet.jpg *License:* CC-BY-3.0 *Contributors:*
I made this. You can make your own at bitcoinpaperwallet.com.
Original artist:
Canton
- **File:ETHEREUM-YOUTUBE-PROFILE-PIC.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/b/b7/ETHEREUM-YOUTUBE-PROFILE-PIC.png> *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Poridge123
- **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 Mecer
- **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_Software_Portal_Logo.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/6/67/Nuvola_apps_emacs_vector.svg *License:* LGPL *Contributors:* Nuvola_apps_emacs.png *Original artist:* Nuvola_apps_emacs.png: David Vignoni
- **File:Mastercoin_logo.png** *Source:* https://upload.wikimedia.org/wikipedia/en/1/17/Mastercoin_logo.png *License:* Fair use *Contributors:* <http://www.mastercoin.org/> *Original artist:* ?
- **File:Mnparpays.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/9/93/Mnparpays.png> *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Tesquenaire
- **File:Monero_XMR_logo.png** *Source:* https://upload.wikimedia.org/wikipedia/en/6/6b/Monero_XMR_logo.png *License:* Fair use *Contributors:* <http://monero.cc/downloads/resources/branding.zip> *Original artist:* ?
- **File:Monero_coin_supply_and_inflation_over_time.png** *Source:* https://upload.wikimedia.org/wikipedia/en/d/db/Monero_coin_supply_and_inflation_over_time.png *License:* Fair use *Contributors:* <https://bitcointalk.org/index.php?topic=583449.msg11342408#msg11342408> *Original artist:* dnaleor
- **File:NEM_logo.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f8/NEM_logo.svg *License:* CC0 *Contributors:* Own work *Original artist:* Mixmaster2
- **File:NEM[?].png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/3/34/NEM%E6%9E%B6%E6%9E%84.png> *License:* CC BY-SA 3.0 *Contributors:* This is a computer drawn illustration diagram *Original artist:* Rockethead123
- **File:Nuvola_apps_kaboodle.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/1b/Nuvola_apps_kaboodle.svg *License:* LGPL *Contributors:* <http://ftp.gnome.org/pub/GNOME/sources/gnome-themes-extras/0.9/gnome-themes-extras-0.9.0.tar.gz> *Original artist:* David Vignoni / ICON KING
- **File:Nxt-logo-vector-yellow.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/5/57/Nxt-logo-vector-yellow.svg> *License:* CC0 *Contributors:* <http://nxtter.org/what-style-is-nxt/> *Original artist:* Ideenfrische
- **File:Nxt_Plugin_for_Crowdfunding_(Alpha).jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/0/09/Nxt_Plugin_for_Crowdfunding_%28Alpha%29.jpg *License:* CC0 *Contributors:* Own work *Original artist:* Screenshot by Thomas Veil
- **File:Nxt_SecureAE_Asset_Exchange_view.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/fb/Nxt_SecureAE_Asset_Exchange_view.png *License:* CC0 *Contributors:* Own work *Original artist:* Thomas Veil
- **File:Nxt_Wallet.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/14/Nxt_Wallet.jpg *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Chilin
- **File:Official_Dash_Logo.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/42/Official_Dash_Logo.png *License:* CC BY-SA 4.0 *Contributors:* <https://www.dashpay.io/promotional-graphics/> *Original artist:* Dash community
- **File:Open_book_icon.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/6/6a/Open_book_icon.png *License:* CC BY-SA 3.0 *Contributors:* Cropped from File:Collection Extension - Create a book box.png *Original artist:* He!ko, Aryamanarora
- **File:Original_Namecoin_Logo.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/94/Original_Namecoin_Logo.png *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* dwda (artisbigshirts)
- **File:PPCoin_Logo_With_Shadow.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/73/PPCoin_Logo_With_Shadow.svg *License:* MIT *Contributors:* <http://sourceforge.net/projects/ppcoin/files/resources/> *Original artist:* Sunny King
- **File:Portal-puzzle.svg** *Source:* <https://upload.wikimedia.org/wikipedia/en/f/fd/Portal-puzzle.svg> *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:PotCoin.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/4/45/PotCoin.png> *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Deemington
- **File:Primecoin_Logo.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/cd/Primecoin_Logo.png *License:* MIT *Contributors:* Primecoin Client *Original artist:* Sunny King
- **File:Proof_of_Work_challenge_response.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/5/55/Proof_of_Work_challenge_response.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **File:Proof_of_Work_solution_verification.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/2/24/Proof_of_Work_solution_verification.svg *License:* PD *Contributors:* ? *Original artist:* ?
- **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:Ripple_logo.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/8/88/Ripple_logo.svg *License:* Public domain *Contributors:* <https://commons.wikimedia.org/wiki/File:Ripple-logo.svg> *Original artist:* Ripple
- **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:Titcoin_Branded_Logo_(Horizontal).png** *Source:* https://upload.wikimedia.org/wikipedia/en/7/72/Titcoin_Branded_Logo_%28Horizontal%29.png *License:* Fair use *Contributors:* <http://www.titcoins.biz/about-us/> *Original artist:* ?
- **File:Titcoin_Coin_Logo.png** *Source:* https://upload.wikimedia.org/wikipedia/en/e/ea/Titcoin_Coin_Logo.png *License:* Fair use *Contributors:* <http://www.titcoins.biz/about-us/> *Original artist:* ?
- **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:Unbalanced_scales.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/fc/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: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:* ? *Original artist:* ?
- **File:Wikibooks-logo-en-noslogan.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/d/df/Wikibooks-logo-en-noslogan.svg> *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* User:Bastique, User:Ramac et al.
- **File:Wikibooks-logo.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/f/fa/Wikibooks-logo.svg> *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* User:Bastique, User:Ramac et al.
- **File:Wikidata-logo.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/f/ff/Wikidata-logo.svg> *License:* Public domain *Contributors:* Own work *Original artist:* User:Planemad
- **File:Wikinews-logo.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/2/24/Wikinews-logo.svg> *License:* CC BY-SA 3.0 *Contributors:* This is a cropped version of Image:Wikinews-logo-en.png. *Original artist:* Vectorized by Simon 01:05, 2 August 2006 (UTC) Updated by Time3000 17 April 2007 to use official Wikinews colours and appear correctly on dark backgrounds. Originally uploaded by Simon.
- **File:Wikiquote-logo.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/f/fa/Wikiquote-logo.svg> *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Wikisource-logo.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/4/4c/Wikisource-logo.svg> *License:* CC BY-SA 3.0 *Contributors:* Rei-artur *Original artist:* Nicholas Moreau
- **File:Wikiversity-logo-Snorky.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/1/1b/Wikiversity-logo-en.svg> *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Snorky
- **File:Wiktionary-logo-en.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/f/f8/Wiktionary-logo-en.svg> *License:* Public domain *Contributors:* Vector version of Image:Wiktionary-logo-en.png. *Original artist:* Vectorized by Fvasconcellos (talk · contribs), based on original logo tossed together by Brion Vibber
- **File:Zerocoin_logo.png** *Source:* https://upload.wikimedia.org/wikipedia/en/4/46/Zerocoin_logo.png *License:* Fair use *Contributors:* <http://zerocoin.org/> *Original artist:* ?

7.3 Content license

- Creative Commons Attribution-Share Alike 3.0