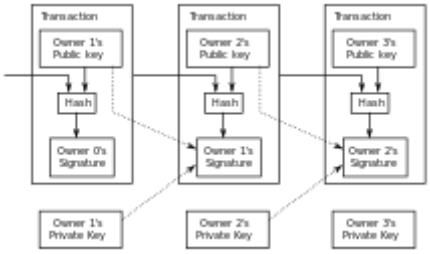
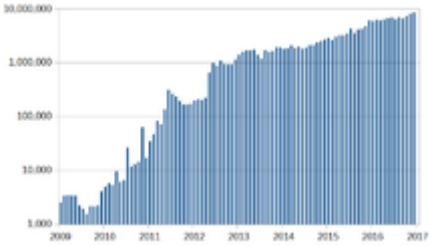
Bitcoin network

The **bitcoin network** is a peer-to-peer payment network that operates on a cryptographic protocol. Users send and receive bitcoins, the units of currency, by broadcasting digitally signed messages to the network using bitcoin cryptocurrency wallet software. Transactions are recorded into a distributed, replicated public database known as the blockchain, with consensus achieved by a proof-of-work system called *mining*. Satoshi Nakamoto, the designer of bitcoin, claimed that design and coding of bitcoin began in 2007. The project was released in 2009 as open source software.



A diagram of a bitcoin transfer

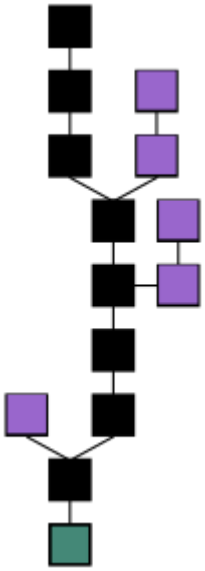
The network requires minimal structure to share transactions. An ad hoc decentralized network of volunteers is sufficient. Messages are broadcast on a best-effort basis, and nodes can leave and rejoin the network at will. Upon reconnection, a node downloads and verifies new blocks from other nodes to complete its local copy of the blockchain.[2][3]



Number of bitcoin transactions per month (logarithmic scale)[1]

Contents

Transactions



The best chain ■ consists of the longest series of transaction records from the genesis block ■ to the current block or record. Orphaned records ■ exist outside of the best chain.

A bitcoin is defined by a sequence of digitally signed transactions that began with the bitcoin's creation, as a block reward. The owner of a bitcoin transfers it by digitally signing it over to the next owner using a bitcoin transaction, much like endorsing a traditional bank check. A payee can examine each previous transaction to verify the chain of ownership. Unlike traditional check endorsements, bitcoin transactions are irreversible, which eliminates risk of chargeback fraud.

An actual bitcoin transaction including the fee from a web-based cryptocurrency exchange to a hardware wallet.

Although it is possible to handle bitcoins individually, it would be unwieldy to require a separate transaction for every bitcoin in a transaction. Transactions are therefore allowed to contain multiple inputs and outputs, allowing bitcoins to be split and combined. Common transactions will have either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and one or two outputs: one for the payment, and one returning the change, if any, to the sender. Any difference between the total input and output amounts of a transaction goes to miners as a transaction fee.[2]

Mining

To form a distributed timestamp server as a peer-to-peer network, bitcoin uses a proof-of-work system.[3] This work is often called *bitcoin mining*.

GPU-based mining rig, 2012

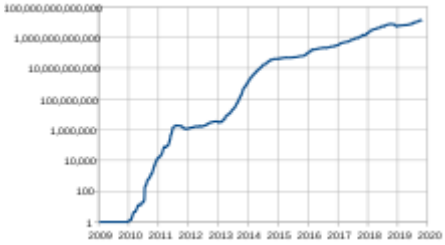
Requiring a proof of work to accept a new block to the blockchain was Satoshi Nakamoto's key innovation. The mining process involves identifying a block that, when hashed twice with SHA-256, yields a number smaller than the given difficulty target. While the average work required increases in inverse proportion to the difficulty target, a hash can always be verified by executing a single round of double SHA-256.

A Bitcoin mining farm, 2018

For the bitcoin timestamp network, a valid proof of work is found by incrementing a nonce until a value is found that gives the block's hash the required number of leading zero bits. Once the hashing has produced a valid result, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing the work for each subsequent block. If there is a deviation in consensus then a blockchain fork can occur.

Majority consensus in bitcoin is represented by the longest chain, which required the greatest amount of effort to produce. If a majority of computing power is controlled by honest nodes, the honest chain will grow fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of that block and all blocks after it and then surpass the work of the honest nodes. The probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.[3]

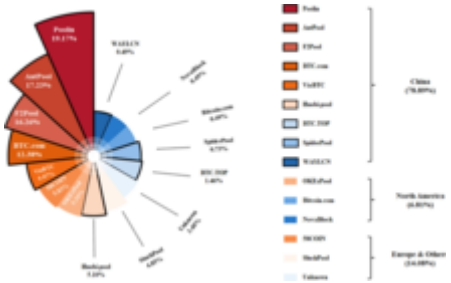
To compensate for increasing hardware speed and varying interest in running nodes over time, the difficulty of finding a valid hash is adjusted roughly every two weeks. If blocks are generated too quickly, the difficulty increases and more hashes are required to make a block and to generate new bitcoins.[3]



Mining difficulty has increased significantly

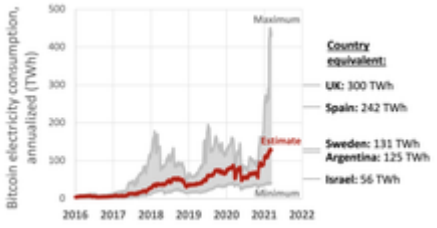
Difficulty and mining pools

Bitcoin mining is a competitive endeavor. An "arms race" has been observed through the various hashing technologies that have been used to mine bitcoins: basic central processing units (CPUs), high-end graphics processing units (GPUs), field-programmable gate arrays (FPGAs) and application-specific integrated circuits (ASICs) all have been used, each reducing the profitability of the less-specialized technology. Bitcoin-specific ASICs are now the primary method of mining bitcoin and have surpassed GPU speed by as much as 300-fold. The difficulty within the mining process involves self-adjusting to the network's accumulated mining power. As bitcoins have become more difficult to mine, computer hardware manufacturing companies have seen an increase in sales of high-end ASIC products.[4]


The largest Bitcoin mining pools as of April 2020 by nation they're based in

Computing power is often bundled together or "pooled" to reduce variance in miner income. Individual mining rigs often have to wait for long periods to confirm a block of transactions and receive payment. In a pool, all participating miners get paid every time a participating server solves a block. This payment depends on the amount of work an individual miner contributed to help find that block.[5]

Energy sources and consumption



Bitcoin electricity consumption as of 2021[6]

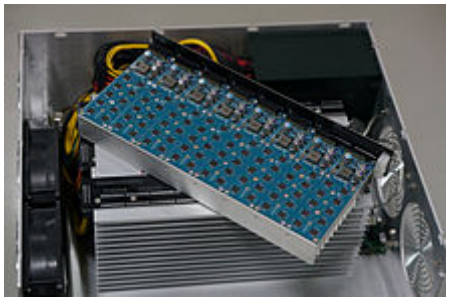
In 2013, Mark Gimein estimated electricity consumption to be about 40.9 megawatts (982 megawatt-hours a day).[7] In 2014, Hass McCook estimated 80.7 megawatts (80,666 kW). As of 2015, *The Economist* estimated that even if all miners used modern facilities, the combined electricity consumption would be 166.7 megawatts (1.46 terawatt-hours per year).[8] The Cambridge Bitcoin Electricity Consumption Index estimates the energy use of the bitcoin network grew from 1.95 terawatt-hours per year at the end of 2014, to 77.1 terawatt-hours per year by the end of 2019.[6]

Seeking lower electricity costs, some bitcoin miners have set up in places like Iceland where geothermal energy is cheap and cooling Arctic air is free.[9] Chinese bitcoin miners are known to use hydroelectric power in Tibet to reduce electricity costs.[10] North American companies are utilizing stranded gas as a cost-effective source of energy for bitcoin mining.[11] In West Texas, wind powers bitcoin mining.[12] As of April 2021, at least one-third of Bitcoin mining was powered by coal in China's Xinjiang region.[13]

A 2021 study found that carbon emissions from Bitcoin mining in China – where a majority of the proof-of-work algorithm that generates current economic value is computed – have accelerated rapidly, are largely fueled by nonrenewable sources and would soon exceed total annual emissions of countries like Italy and Spain during 2016, interfering with international climate change mitigation commitments.[14][15]

Process

A rough overview of the process to mine bitcoins involves:[3]



Avalon ASIC-based mining machine

1. New transactions are broadcast to all nodes.
2. Each miner node collects new transactions into a block.
3. Each miner node works on finding a proof-of-work code for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Receiving nodes validate the transactions it holds and accept only if all are valid.
6. Nodes express their acceptance by moving to work on the next block, incorporating the hash of the accepted block.

Mined bitcoins

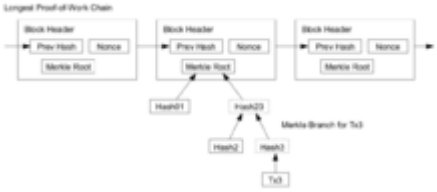


Diagram showing how bitcoin transactions are verified

By convention, the first transaction in a block is a special transaction that produces new bitcoins owned by the creator of the block. This is the incentive for nodes to support the network.[2] It provides the way to move new bitcoins into circulation. The reward for mining halves every 210,000 blocks. It started at 50 bitcoin, dropped to 25 in late 2012 and to 12.5 bitcoin in 2016. The most recent halving, which occurred in May 2020 (with block number 630,000), reduced the block reward to 6.25 bitcoin. This halving process is programmed to continue a maximum 64 times before new coin creation ceases.[16]

Security

Various potential attacks on the bitcoin network and its use as a payment system, real or theoretical, have been considered. The bitcoin protocol includes several features that protect it against some of those attacks, such as unauthorized spending, double spending, forging bitcoins, and tampering with the blockchain. Other attacks, such as theft of private keys, require due care by users.[17][18]

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 blockchain) that is visible to all users, and ensuring for all transferred bitcoins that they have not 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 blockchain.[19]

A variant race attack (which has been called a Finney attack by reference to Hal Finney) requires the participation of a miner. Instead of sending both payment requests (to pay Bob and Alice with the same coins) to the network, Eve issues only Alice's payment request to the network, while the accomplice tries to mine a block that includes the payment to Bob instead of Alice. There is a positive probability that the rogue miner will succeed before the network, in which case the payment to Alice will be rejected. As with the plain race attack, Alice can reduce the risk of a Finney attack by waiting for the payment to be included in the blockchain.[20]

History modification

Each block that is added to the blockchain, starting with the block containing a given transaction, is called a confirmation of that transaction. Ideally, merchants and services that receive payment in bitcoin should wait for at least one confirmation to be distributed over the network, before assuming that the payment was done. The more confirmations that the merchant waits for, the more difficult it is for an attacker to successfully reverse the transaction in a blockchain—unless the attacker controls more than half the total network power, in which case it is called a 51% attack.[21]

Deanonymisation of clients

Deanonymisation is a strategy in data mining in which anonymous data is cross-referenced with other sources of data to re-identify the anonymous data source. Along with transaction graph analysis, which may reveal connections between bitcoin addresses (pseudonyms),[17][22] there is a possible attack[23] which links a user's pseudonym to its IP address. If the peer is using Tor, the attack includes a method to separate the peer from the Tor network, forcing them to use their real IP address for any further transactions. The attack makes use of bitcoin mechanisms of relaying peer addresses and anti-DoS protection. The cost of the attack on the full bitcoin network is under €1500 per month.[23]

Payment verification

Each miner can choose which transactions are included in or exempted from a block.[24] A greater number of transactions in a block does not equate to greater computational power required to solve that block.[24]

Upon receiving a new transaction a node must validate it: in particular, verify that none of the transaction's inputs have been previously spent. To carry out that check, the node needs to access the blockchain. Any user who does not trust his network neighbors, should keep a full local copy of the blockchain, so that any input can be verified.

As noted in Nakamoto's whitepaper, it is possible to verify bitcoin payments without running a full network node (simplified payment verification, SPV). A user only needs a copy of the block headers of the longest chain, which are available by querying network nodes until it is apparent that the longest chain has been obtained; then, get the Merkle tree branch linking the transaction to its block. Linking the transaction to a place in the chain demonstrates that a network node has accepted it, and blocks added after it further establish the confirmation.[2]

Data in the blockchain

While it is possible to store any digital file in the blockchain, the larger the transaction size, the larger any associated fees become. Various items have been embedded, including URLs to websites, an ASCII art image of Ben Bernanke, material from the Wikileaks cables, prayers from bitcoin miners, and the original bitcoin whitepaper.[25]

Alleged criminal activity

The use of bitcoin by criminals has attracted the attention of financial regulators, legislative bodies, law enforcement, and the media.[26] The FBI prepared an intelligence assessment,[27] the SEC has issued a pointed warning about investment schemes using virtual currencies,[26] and the U.S. Senate held a hearing on virtual currencies in November 2013.[28]

Several news outlets have asserted that the popularity of bitcoins hinges on the ability to use them to purchase illegal goods.[29][30] 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."[31]

Black markets

A Carnegie Mellon University 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 dark web drugs market, Silk Road.[32] Child pornography,[33] murder-for-hire,[34] and weapons[35] 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.[36]

Several deep web black markets have been shut by authorities. In October 2013 Silk Road was shut down by U.S. law enforcement,[37][38][39] leading to a short-term decrease in the value of bitcoin.[40] In 2015, the founder of the site was sentenced to life in prison.[41] 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.[42] In early 2014, Dutch authorities closed Utopia, an online illegal goods market, and seized 900 bitcoins.[43] 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.[44] 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,[45] and in February 2015, its founder, Ross Ulbricht, was convicted on drugs charges and given a sentence of double life imprisonment plus 40 years.[46]

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.[47] In a separate case, escrow accounts with bitcoins belonging to patrons of a different black market were hacked in early 2014.[48]

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 is not 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.[33] Some of these sites have shut down, such as a deep web crowdfunding website that aimed to fund the creation of new child porn.[49] Furthermore, hyperlinks to child porn websites have been added to the blockchain as arbitrary data can be included when a transaction is made.[50][51]

Money laundering

Bitcoins may not be ideal for money laundering, because all transactions are public.[52] Authorities—including the European Banking Authority,[53] the FBI,[27] South African Reserve Bank and the Financial Action Task Force of the G7[54]—have expressed concerns that bitcoin may be used for money laundering. In early 2014, an operator of a U.S. bitcoin exchange, Charlie Shrem, was arrested for money laundering.[55] Subsequently, he was sentenced to two years in prison for "aiding and abetting an unlicensed money transmitting business".[45] Alexander Vinnik, an alleged owner of BTC-e, was arrested in Greece on July 25, 2017, on $4 billion money laundering charges for flouting anti-money laundering (AML) laws of the US. A report by the UK's Treasury and Home Office named "UK national risk assessment of money laundering and terrorist financing" (October 2015) found that, of the twelve methods examined in the report, bitcoin carries the lowest risk of being used for money laundering, with the most common money laundering method being the banks.[56]

Ponzi scheme

In a Ponzi scheme using bitcoins, the Bitcoin Savings and Trust promised investors up to 7% weekly interest, and raised at least 700,000 bitcoins from 2011 to 2012.[57] 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".[57] In September 2014 the judge fined Bitcoin Savings & Trust and its owner $40 million.[58]

See also

- Lists of network protocols
- List of bitcoin organizations
- Economics of bitcoin

References

1. "Charts" (https://blockchain.info/charts). Blockchain.info. Archived (https://web.archive.org/web/20141103020741/http://blockchain.info/charts) from the original on 3 November 2014. Retrieved 2 November 2014.
2. Nakamoto, Satoshi (24 May 2009). "Bitcoin: A Peer-to-Peer Electronic Cash System" (https://bitcoin.org/bitcoin.pdf) (PDF). Retrieved 20 December 2012.

3. Barber, Simon; Boyen, Xavier; Shi, Elaine & Uzun, Ersin (2012). "Bitter to Better – how to make Bitcoin a better currency" (http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf) (PDF). *Financial Cryptography and Data Security*. Lecture Notes in Computer Science. Springer Publishing. **7397**: 399–414. doi:10.1007/978-3-642-32946-3_29 (https://doi.org/10.1007%2F978-3-642-32946-3_29). ISBN 978-3-642-32945-6.
4. "Bitcoin boom benefiting TSMC: report" (http://www.taipeitimes.com/News/biz/archives/2014/01/04/2003580449). *Taipei Times*. 4 January 2014.
5. Biggs, John (8 April 2013). "How To Mine Bitcoins" (https://techcrunch.com/2013/04/08/how-to-mine-bitcoins/). Techcrunch.
6. "Cambridge Bitcoin Electricity Consumption Index (CBECI)" (https://www.cbeci.org/). *www.cbeci.org*. Retrieved 20 February 2020.
7. Gimein, Mark (13 April 2013). "Virtual Bitcoin Mining Is a Real-World Environmental Disaster" (https://www.bloomberg.com/news/articles/2013-04-12/virtual-bitcoin-mining-is-a-real-world-environmental-disaster). *Bloomberg Business*. Bloomberg LP. Retrieved 22 April 2015.
8. "The magic of mining" (https://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic). *The Economist*. 13 January 2015. Retrieved 13 January 2015.
9. O'Brien, Matt (13 June 2015). "The scam called Bitcoin" (http://www.dailyherald.com/article/20150613/business/150619551/). *Daily Herald*. Retrieved 20 September 2016.
10. Potenza, Alessandra (21 December 2017). "Can renewable power offset bitcoin's massive energy demands?" (https://www.theverge.com/2017/12/21/16806772/bitcoin-cryptocurrency-energy-consumption-renewables-climate-change). *TheVerge News*. Archived (https://web.archive.org/web/20180112155940/https://www.theverge.com/2017/12/21/16806772/bitcoin-cryptocurrency-energy-consumption-renewables-climate-change) from the original on 12 January 2018. Retrieved 12 January 2018.
11. Yang, Stephanie (29 March 2019). "Bitcoin in the wilderness" (https://www.wsj.com/articles/bitcoin-in-the-wilderness-11553860802). *The Wall Street Journal*. Retrieved 29 April 2020.
12. Orcutt, Mike (27 February 2020). "How Texas's wind boom has spawned a Bitcoin mining rush" (https://www.technologyreview.com/2020/02/27/905626/how-texass-wind-boom-has-spawned-a-bitcoin-mining-rush/). *MIT Technology Review*. Retrieved 29 April 2020.
13. "Commentary: How much Bitcoin comes from dirty coal? A flooded mine in China just spotlighted the issue" (https://fortune.com/2021/04/20/bitcoin-mining-coal-china-environment-pollution/). *Fortune*. Retrieved 8 May 2021.
14. Lu, Donna. "Bitcoin mining emissions in China will hit 130 million tonnes by 2024" (https://www.newscientist.com/article/2273672-bitcoin-mining-emissions-in-china-will-hit-130-million-tonnes-by-2024/). *New Scientist*. Retrieved 9 May 2021.
15. Jiang, Shangrong; Li, Yuze; Lu, Quanying; Hong, Yongmiao; Guan, Dabo; Xiong, Yu; Wang, Shouyang (6 April 2021). "Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China" (https://www.nature.com/articles/s41467-021-22256-3). *Nature Communications*. **12** (1): 1938. doi:10.1038/s41467-021-22256-3 (https://doi.org/10.1038%2Fs41467-021-22256-3). ISSN 2041-1723 (https://www.worldcat.org/issn/2041-1723). Retrieved 9 May 2021. Available under CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/).
16. Antonopoulos, Andreas M. (2017). *Mastering Bitcoin : programming the open blockchain* (Second ed.). Sebastopol, CA. p. 239. ISBN 978-1-4919-5438-6. OCLC 953432201 (https://www.worldcat.org/oclc/953432201).
17. Ron Dorit; Adi Shamir (2012). "Quantitative Analysis of the Full Bitcoin Transaction Graph" (http://eprint.iacr.org/2012/584.pdf) (PDF). Cryptology ePrint Archive. Retrieved 18 October 2012.

18. Jerry Brito & Andrea Castillo (2013). "Bitcoin: A Primer for Policymakers" (http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf) (PDF). *Mercatus Center*. George Mason University. Retrieved 22 October 2013.
19. Erik Bonadonna (29 March 2013). "Bitcoin and the Double-spending Problem" (http://blogs.cornell.edu/info4220/2013/03/29/bitcoin-and-the-double-spending-problem/). Cornell University. Retrieved 22 October 2014.
20. Karame, Ghassan O.; Androulaki, Elli; Capkun, Srdjan (2012). "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin" (http://eprint.iacr.org/2012/248.pdf) (PDF). International Association for Cryptologic Research. Retrieved 22 October 2014.
21. Michael J. Casey; Paul Vigna (16 June 2014). "Short-Term Fixes To Avert "51% Attack" " (https://blogs.wsj.com/moneybeat/2014/06/16/bitbeat-a-51-attack-what-is-it-and-could-it-happen/). *Money Beat*. Wall Street Journal. Retrieved 30 June 2014.
22. Reid, Fergal; Harrigan, Martin (2013). "An Analysis of Anonymity in the Bitcoin System". *Security and Privacy in Social Networks*: 197–223. arXiv:1107.4524 (https://arxiv.org/abs/1107.4524). doi:10.1007/978-1-4614-4139-7_10 (https://doi.org/10.1007%2F978-1-4614-4139-7_10). ISBN 978-1-4614-4138-0.
23. Biryukov, Alex; Khovratovich, Dmitry; Pustogarov, Ivan (2014). "Deanonymisation of clients in Bitcoin P2P network" (http://orbilu.uni.lu/handle/10993/18679). *ACM Conference on Computer and Communications Security*. arXiv:1405.7418 (https://arxiv.org/abs/1405.7418). Bibcode:2014arXiv1405.7418B (https://ui.adsabs.harvard.edu/abs/2014arXiv1405.7418B).
24. Houy, N. (2016). "The Bitcoin Mining Game" (http://www.ledgerjournal.org/ojs/index.php/ledger/article/view/13/59). *Ledger*. **1**: 53–68. doi:10.5195/ledger.2016.13 (https://doi.org/10.5195%2Fledger.2016.13). Retrieved 14 January 2017.
25. "How porn links and Ben Bernanke snuck into Bitcoin's code" (https://money.cnn.com/2013/05/02/technology/security/bitcoin-porn/). *CNN Money*. CNN. 2 May 2013.
26. Lavin, Tim (8 August 2013). "The SEC Shows Why Bitcoin Is Doomed" (http://www.bloombergview.com/articles/2013-08-08/did-the-sec-just-validate-bitcoin-no-). *bloomberg.com*. Bloomberg LP. Retrieved 20 October 2013.
27. "Bitcoins Virtual Currency: Unique Features Present Challenges for Deterring Illicit Activity" (https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf) (PDF). *Cyber Intelligence Section and Criminal Intelligence Section*. FBI. 24 April 2012. Retrieved 2 November 2014.
28. Lee, Timothy B. (21 November 2013). "Here's how Bitcoin charmed Washington" (https://www.washingtonpost.com/news/the-switch/wp/2013/11/21/heres-how-bitcoin-charmed-washington/). *The Washington Post*. Retrieved 10 October 2016.
29. "Monetarists Anonymous" (http://www.economist.com/node/21563752). *The Economist*. The Economist Newspaper Limited. 29 September 2012. Retrieved 21 October 2013.
30. Ball, James (22 March 2013). "Silk Road: the online drug marketplace that officials seem powerless to stop" (https://www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace). *theguardian.com*. Guardian News and Media Limited. Retrieved 20 October 2013.
31. Matthew Graham Wilson & Aaron Yelowitz (November 2014). "Characteristics of Bitcoin Users: An Analysis of Google Search Data". *Social Science Research Network*. Working Papers Series. SSRN 2518603 (https://ssrn.com/abstract=2518603).

32. Christin, Nicolas (2013). *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace* (http://www.andrew.cmu.edu/user/nicolasc/publications/Christin-WWW13.pdf) (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"
33. Schweizer, Kristen (10 October 2014). "Bitcoin Payments by Pedophiles Frustrate Child Porn Fight" (https://www.bloomberg.com/news/articles/2014-10-09/bitcoin-payments-by-pedophiles-frustrate-child-porn-fight). *BloombergBusiness*. Bloomberg LP. Retrieved 16 February 2015.
34. Lake, Eli (17 October 2013). "Hitman Network Says It Accepts Bitcoins to Murder for Hire" (http://www.thedailybeast.com/articles/2013/10/17/hitman-network-says-it-accepts-bitcoins-to-murder-for-hire.html). *The Daily Beast*. The Daily Beast Company LLC. Retrieved 17 February 2015.
35. Smith, Gerry (15 April 2013). "How Bitcoin Sales Of Guns Could Undermine New Rules" (http://www.huffingtonpost.com/2013/04/15/bitcoin-guns_n_3070828.html). *huffingtonpost.com*. TheHuffingtonPost.com, Inc. Retrieved 20 October 2013.
36. Alex, Knapp (19 January 2015), "Faking Murders And Stealing Bitcoin: Why The Silk Road Is The Strangest Crime Story Of The Decade" (https://www.forbes.com/sites/alexknapp/2015/01/19/faking-murders-and-stealing-bitcoin-why-the-silk-road-is-the-strangest-crime-story-of-the-decade/), *Forbes*, retrieved 2 January 2016
37. Andy Greenberg (23 October 2013). "FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road" (https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/) (blog). *Forbes.com*. Retrieved 24 November 2013.
38. Kelion, Leo (12 February 2014). "Five arrested in Utopia dark net marketplace crackdown" (https://www.bbc.co.uk/news/technology-26158012). *bbc.co.uk*. BBC. Retrieved 13 February 2014.
39. Alex Hern (3 October 2013). "Bitcoin price plummets after Silk Road closure" (https://www.theguardian.com/technology/2013/oct/03/bitcoin-price-silk-road-ulbricht-value). *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"
40. Robert McMillan (2 October 2013). "Bitcoin Values Plummet $500M, Then Recover, After Silk Road Bust" (https://www.wired.com/2013/10/bitcoin-market-drops-600-million-on-silk-road-bust/). *Wired*. Retrieved 31 October 2014.
41. "Silk Road drug website founder Ross Ulbricht jailed" (https://www.bbc.com/news/world-us-canada-32941060). *BBC News*. BBC. 29 May 2015. Retrieved 30 May 2015.
42. Katie Silver (31 March 2014). "Silk Road closure fails to dampen illegal drug sales online, experts say" (http://www.abc.net.au/news/2014-03-31/online-drug-trade-soaring-experts-say/5354930). *ABC News*. Retrieved 31 October 2014.
43. Sophie Murray-Morris (13 February 2014). "Utopia no more: Drug marketplace seen as the next Silk Road shut down by Dutch police" (https://www.independent.co.uk/life-style/gadgets-and-tech/utopia-no-more-drug-marketplace-seen-as-the-next-silk-road-shut-down-by-dutch-police-9126063.html). *The Independent*. London: independent.co.uk. Retrieved 8 November 2014.
44. Wakefield, Jane (7 November 2014). "Huge raid to shut down 400-plus dark net sites" (https://www.bbc.com/news/technology-29950946). *bbc.com*. BBC. Retrieved 8 November 2014.

45. Nate Raymond (19 December 2014). "Bitcoin backer gets two years prison for illicit transfers" (https://www.reuters.com/article/us-usa-crime-bitcoin-idUSKBN0JX2CW20141219). *Reuters*. Thompson Reuters. Archived (https://web.archive.org/web/20151113195704/http://www.reuters.com/article/2014/12/19/us-usa-crime-bitcoin-idUSKBN0JX2CW20141219) from the original on 13 November 2015. Retrieved 20 December 2014.
46. "Ross Ulbricht: Silk Road creator convicted on drugs charges" (https://www.bbc.com/news/world-us-canada-31134938). BBC. 5 February 2015. Retrieved 17 February 2015.
47. Ravi Mandalia (1 December 2013). "Silk Road-like Sheep Marketplace scams users; over 39k Bitcoins worth $40 million stolen" (http://www.techienews.co.uk/973470/silk-road-like-sheep-marketplace-scams-users-39k-bitcoins-worth-40-million-stolen/). Techie News. Retrieved 2 December 2013.
48. "Silk Road 2 loses $2.7m in bitcoins in alleged hack" (https://www.bbc.co.uk/news/technology-26187725). *BBC News*. 14 February 2014. Retrieved 15 February 2014.
49. "While Markets Get Seized: Pedophiles Launch a Crowdfunding Site" (https://web.archive.org/web/20150208050521/http://www.deepdotweb.com/2014/11/09/as-drug-markets-are-seized-pedophiles-launch-a-crowdfunding-site/). Archived from the original (http://www.deepdotweb.com/2014/11/09/as-drug-markets-are-seized-pedophiles-launch-a-crowdfunding-site/) on 8 February 2015. Retrieved 19 February 2015.
50. Hopkins, Curt (7 May 2013). "If you own Bitcoin, you also own links to child porn" (http://www.dailydot.com/business/bitcoin-child-porn-transaction-code/). *The Daily Dot*. Retrieved 16 February 2015.
51. Bradbury, Danny. "As Bitcoin slides, the Blockchain grows" (https://web.archive.org/web/20160830144934/http://eandt.theiet.org/magazine/2015/02/in-blocks-we-trust.cfm). IET Engineering and Technology Magazine. Archived from the original (http://eandt.theiet.org/magazine/2015/02/in-blocks-we-trust.cfm) on 30 August 2016.
52. Kirk, Jeremy (28 August 2013). "Bitcoin offers privacy-as long as you don't cash out or spend it" (http://www.pcworld.com/article/2047608/bitcoin-offers-privacy-as-long-as-you-dont-cash-out-or-spend-it.html). *PC World*. Retrieved 31 October 2014.
53. "Warning to consumers on virtual currencies" (https://web.archive.org/web/20131224121925/http://www.eba.europa.eu/documents/10180/16136/EBA+Warning+on+Virtual+Currencies.pdf) (PDF). European Banking Authority. 12 December 2013. Archived from the original (http://www.eba.europa.eu/documents/10180/16136/EBA+Warning+on+Virtual+Currencies.pdf) (PDF) on 24 December 2013. Retrieved 23 December 2013.
54. "Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services" (http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf) (PDF). *Guidance for a risk-based approach*. Paris: Financial Action Task Force (FATF). June 2013. p. 47. Retrieved 6 March 2014.
55. Lee, Dave (27 January 2014). "US makes Bitcoin exchange arrests after Silk Road closure" (https://www.bbc.co.uk/news/technology-25919482). *bbc.co.uk*. BBC. Retrieved 28 January 2014.
56. "UK national risk assessment of money laundering and terrorist financing" (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf) (PDF). UK HM Treasury and Home Office. Retrieved 3 May 2016.
57. "SEC charges Texas man with running Bitcoin-denominated Ponzi scheme" (https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539730583) (Press release). US Securities and Exchange Commission. 23 July 2013. Retrieved 7 March 2014.
58. Jay Adkisson (25 September 2014). "Bitcoin Savings & Trust Comes Up $40 Million Short On The Trust Part" (https://www.forbes.com/sites/jayadkisson/2014/09/25/bitcoin-savings-trust-comes-up-40-million-short-on-the-trust-part). *Forbes*. Retrieved 13 December 2014.
