



# Authority Printed Upon Emptiness

Kieron O'Hara • University of Southampton

In 2014, two European nations, Russia and Ukraine, began an unofficial war, leading to sanctions. Unsurprisingly, their respective currencies (the rouble and the hryvnia) tanked. Yet they weren't the worst-performing currencies of 2014 – that award went to bitcoin. Bitcoin ended 2013 at extraordinary highs – often in excess of US\$900 and reaching \$1,100. By January 2015 it was below \$300 (at the time of writing, about \$266). In contrast, the rouble and the hryvnia lost a mere 50 percent or so of their value.

Yet bitcoin continues to be lionized by its many fans. And 2014 was its *annus horribilis*, with the MtGox scandal, problems with other exchanges, a minor regulatory crackdown in bitcoin-crazy China, and the arrest of Silk Road's Dread Pirate Roberts. Nevertheless, in 2015 the Greek government's tribulations as it struggled to adapt to its commitments to the euro suggested to some that bitcoins could be the solution to its problems. Libertarian economic theorists like Friedrich Hayek have long advocated creating sound money by decoupling the money supply from spendthrift national governments,<sup>1</sup> while the abolition of cash and a permanent move to digital money is increasingly advocated.<sup>2</sup> A decentralized, independent, non-inflationary, foolproof digital currency – what's not to like?

### What It Does and What It Is

The peer-to-peer (P2P) design of bitcoin<sup>3</sup> is undoubtedly brilliant in its solutions to three problems. The first is that of authenticity assurance: Can we avoid counterfeiting? Bitcoin, like other digital currencies, uses cryptography and digital signatures to show legitimacy. Second, we need to avoid double spending: Can we prevent people spending the same bitcoin twice?

Yes, again by using verified signatures. The database that prevents double-spending isn't centrally controlled, and so bitcoin avoids creating the bottlenecks that allow rent-seeking on the part of banks and clearing houses. Third, can the currency be made robust against inflation? Once more, yes – and this is the clever part – by cutting governments, banks, and other central authorities out of the loop, and instead distributing power over the bitcoin network.

The number of bitcoins that can ever appear is limited to 21 million, and so it functions rather like the gold standard or a currency peg, which restrain inflation via restrictive supply of the underlying source of value. However, a decision to use gold as a basis for a currency is a government decision. Governments therefore aren't taken out of the loop by such measures, and can decide to come off standards and pegs as easily as adopting them, as they have done in expensive times of crisis such as World War I, the Great Depression, the Vietnam War, and the financial crises of 1997–1999. Bitcoin being a P2P system, governments play no role, people use it if both sides of the exchange agree, and no one can decide to mine more bitcoins than expected. A government might decide to adopt bitcoin as a national currency, or peg its own currency to the bitcoin, but – although it would have far-reaching consequences for the nation – this would have no effect on bitcoin itself. However, at the moment this is an extremely unlikely scenario, as I will explain.

Bitcoin has five key components.<sup>4</sup>

- First, there's a decentralized P2P network connected by the bitcoin protocol, consisting of nodes that play a number of roles. Nodes are able to validate transactions and records of transactions (*blocks*), discover peers in the

network, and maintain communications with them, especially by propagating verified transactions and blocks.

- Second, there's a complete public ledger of all bitcoin transactions (the *blockchain*).
- Third, there's a decentralized scheme for creating bitcoins and creating new additions to the blockchain every 10 minutes or so, based on solving a puzzle that demands a brute-force approach (*mining*).
- Fourth, there's a proof-of-work algorithm to show that the latest block on the chain has been correctly mined.
- And finally, there's a decentralized transaction verification scheme.

These are connected by carefully calibrated incentives and reciprocity between network nodes. A node may contain a *wallet*, which points to the transactions in the blockchain that contain unspent payments to its owner. If the node is a *miner*, then it will contain specialized software, and more likely hardware, to compete with other miners to solve the mining puzzle. Some nodes contain complete copies of the entire blockchain, which date back to the so-called genesis block created in January 2009, and which at the time of writing is about 30 gigabytes in size. These can independently verify any transaction by tracing back the history of all transactions of the bitcoin in question to its creation. It's more usual for nodes (in particular, those running on smartphones) to contain an edited version of the latest blocks on the blockchain, and these therefore require outside help to verify a transaction.

## What Does Money Do and Does Bitcoin Do It?

There are two ways of considering bitcoin: as a currency, or as a brilliantly engineered solution to issues

of ownership more widely. Its future may be as the latter rather than the former, but that's not my topic here. In this piece, I focus primarily on bitcoin as the most advanced and capitalized of the cryptocurrencies, but of course we should remember that bitcoin is a prominent exemplar of a set of technologies of which perhaps the distributed verification of proof of work embodied in the blockchain may end up being the most influential. Bitcoin may die, and be replaced by altcoins or altchains, but its principles will remain relevant in many other contexts.

Bitcoin may revert to a value of zero.<sup>5</sup> But as it is used, and as long as it is used for exchange, let's not kid ourselves that bitcoin isn't money. We shouldn't hold its intangible nature against it; as Norman Mailer once put it, all money is "authority printed upon emptiness."<sup>6</sup> It's surely not, as many have claimed, a fraudulent Ponzi scheme,<sup>7</sup> if for no other reason than it promises no profit. Its main advantage might be facilitating the purchase of drugs online, but it does at least some of the legitimate business that we expect from currencies. More precisely, of the three tasks that a currency is supposed to do, it performs one very well while lagging on the other two.

First of all, money is a medium of exchange that we can swap for goods and services. That means it needs to be trusted sufficiently to be used within an economy. Clearly bitcoin does this, as we can buy things with it (some of them are even legal). It's a highly efficient mechanism. The technical infrastructure means that the transaction costs are minimal compared to those of the centralized clearing houses required for bonds or credit cards. The unanswered question is whether the necessary systemic trust could be so widespread that bitcoins become as ubiquitous as (say) credit cards are in Europe or the US. Can bitcoin retain its credibility if it's perpetually caught

up in scandals such as MtGox and Silk Road (even given that its design is only indirectly implicated in these, if at all)?

Second, money is a unit of account. A monetary unit serves as the standard for the value of an economy, company, person, or object. Bitcoin hasn't reached this point yet in the real world – no one claims that her company has a turnover of BTC1,000, or that such-and-such a country has a gross domestic product (GDP) of BTC1,000,000. It's rather counterintuitive to account for very large numbers, given that its market value is in the tens of billions of dollars, and that there's an upper limit to the number in circulation. A nation's GDP might easily exceed the total bitcoin money supply. That's not in itself contradictory, but sounds odd. Bitcoin is equipped to be a unit of account, but in practice nobody uses it in that way. The underlying reason for this is because of its failure to achieve the third function of money.

That third function is that money stores value – I can do some work today, be paid, and reap the reward of my work tomorrow or far into the future. Once more, bitcoin can do this, but not particularly well. I can use the bitcoins in my wallet for purchases or exchange in the future, but their value in terms of goods or other currencies is currently prone to violent fluctuations, so that its use in this way is highly risky. In 2015, at the time of writing, its value against the dollar has swung between \$200 and \$300 – that's pretty violent, but nothing compared to its movements in 2013 and 2014. Anyone who invested in bitcoins prior to 2013 has made an enormous profit, even if they didn't cash in at the top, but someone investing now could easily lose heavily. The uncertainty and volatility make bitcoin currently unsuitable to be a financial frame of reference. Even the most profligate

governments rarely produce currencies as volatile as bitcoin, which is why we won't see bitcoin as a national currency any time soon.

### Inflation — Boo!

As previously noted, there's a theoretical maximum number of bitcoins. Even this number won't effectively be reached, because although lost bitcoins remain evident in the blockchain, they're unusable if proof of ownership can't be provided (as an unfortunate Welshman discovered when he threw away the hard disc of his laptop, forgetting it contained the private key to his wallet — he lost 7,500 of them).<sup>8</sup> It has been calculated that 30 percent of the 14 million existing bitcoins are “zombie” bitcoins that haven't been touched for a year and a half (in some cases because owners have died and not passed on their keys).<sup>9</sup> MtGox managed to misplace 650,000 of them.<sup>10</sup>

Once the maximum number of bitcoins has been mined, it will be inherently deflationary, which many commentators, especially small-government libertarian types, find attractive.<sup>11</sup> Yet inflation has its uses, as Yanis Varoufakis, Greece's former Finance Minister (an unorthodox economist, politically less than astute, impeccably cool) argued in a critique of bitcoin: “there can be no de-politicised currency capable of ‘powering’ an advanced, industrial society.”<sup>12</sup> It's no accident that the gold standard was created at a time when political power largely rested with the creditor class, which naturally wishes to preserve the soundness of money, and it became unsustainable as power shifted in a democratic direction away from the relatively small number of lenders to the larger number of net borrowers.

A deflationary currency would be unattractive in a democratic age because inflation is an important means of reducing debt. Varoufakis was widely reported to have

proposed Greece's adoption of bitcoin if it was forced out of the Eurozone, but this was simply a delicious April Fool gag.<sup>13</sup> If Greece can't default (as Varoufakis and the governing Syriza party would like, in the face of North European opposition), it can realistically only reduce its colossal debt with a currency that it can print (like the old drachma, which it abandoned in 2002). Even the euro is better than bitcoin for that purpose, as the euro could inflate, though it currently shows no sign of doing so.

There are other, better reasons to prefer low inflation to deflation. During a deflationary period, the value of cash increases, and so it becomes rational to hoard it, keeping it out of the real economy and thereby reducing demand, output, and employment. In hard times, it's easier to adjust wages downward by increasing them below the level of inflation, than actively to cut them in nominal terms. Cryptocurrency fans don't trust the independence of central banks, but bankers pursue positive inflation targets for good reason.

### In Many, One

For many, the beauty of bitcoin lies in decentralization. Yet it's remarkable how centralized ownership of bitcoins is.<sup>14</sup> Bitcoin's original architect Satoshi Nakamoto owns at least 7.5 percent of them — although many of these are untouched, and so may be lost.<sup>15</sup> Early adopters own a large fraction, and I wonder how far they could sway markets if they chose to act in a concerted way.

Perhaps a greater concern is the evolution of the mining industry, and how far it has moved away from what *The Economist* called “Mr Nakamoto's libertarian dream: home-brewed money.”<sup>16</sup> In the early days, you really could mine a few bitcoins yourself on a machine, but now the mining business is a boom area in IT, boosted when it moved from software to

specialized hardware; the capacities of application-specific integrated circuits (ASICs) for mining are increasing more quickly than Moore's law, and designs become obsolete in months. In the same way that physical resource mining evolved from the individualistic 49ers to a global industry dominated by three or four megacorps, bitcoin mining now exploits economies of scale. Miners combine their efforts, joining cooperative pools with their own proof-of-work algorithms via which they share their gains. Risk is distributed, while computing power is amalgamated. So massive is the industry that the environment is coming into play as a factor; giant banks of machines need large quantities of electricity and major cooling facilities.

The lesson of the California gold rush was that the people who really get rich often aren't the miners, but those who sell the picks and shovels. Mining capacity can be rented from the cloud in gigahashes per second. Genesis Mining ([www.genesis-mining.com](http://www.genesis-mining.com)) offers “the easiest way of mining: no need to assemble rigs or to have hot, loud miners in your home. ... Start making profit today!” And you know there's money to be made when cybercriminals muscle in; devices on the Internet of Things have been suborned to work on cryptocurrency mining.<sup>17,18</sup>

As with shale oil in the US, the industry invested when the price was high. The collapse in the oil price is producing a shake-out in fracking, and there's no reason to think that the collapse in bitcoin values won't also result in firms exiting the market. Furthermore, the difficulty of the puzzles miners have to solve is a function of the computing power currently working on the system, which is why it has increased by four orders of magnitude since the introduction of mining ASICs.<sup>16</sup> It isn't hard to imagine a world in which there's less competition to solve easier problems,

and this could be exacerbated when the maximum number of bitcoins has been mined – a less certain economy in which miners will have to live off tips from those making transactions or exploiting the blockchain.

This matters, because the P2P system works on consensus and majority opinion. Changes to software, for instance, happen when a large majority of nodes in the network install the update. At the time of writing, a *fork* (a bifurcation of the blockchain) has been introduced thanks to a dispute, as much ideological as technical, over whether to increase block size to expand the system's capacity; whether Bitcoin XT becomes the system's governing software will ultimately be resolved by a consensus that is currently elusive.<sup>19,20</sup> Might far-reaching change be forced through by an intransigent majority? Such a 51 percent attack would certainly be costly, and the hope is it would be prohibitively so. Yet the likely cost is coming down; in 2014 a prominent mining pool was pressured into releasing a denial that it had ambitions to launch such an attack, after having achieved 50 percent of global mining capacity.<sup>21</sup>

In practice, the problem isn't likely to be with a pool of miners that wishes to dominate the system – such pools may come into existence, but they have an interest in perpetuating the decentralized arrangement. Yet the forces in play here aren't all individual self-interests. In 2015, some 80 percent of bitcoin transactions were in the Chinese yuan. Perhaps, following currency controls and a recent drive against corruption, some of these bitcoins are being used to take wealth out of China. If that continues, it will surely provoke some kind of response from the Chinese government, which might be aggressive, but it might be to co-opt the system.

Could that work? Well, the origin of a lot of current mining power is

unknown, but anecdotally there's enormous growth in Inner Mongolia.<sup>22</sup> Why? Because the fact that the bitcoin puzzle needs to be solved with brute force gives a competitive advantage to places with a decent infrastructure and cheap power.<sup>23</sup> Large nations with abundant electricity, technological sophistication, a political agenda, and proud nationalists whose motivations aren't grounded solely in economic self-interest – think China, Russia, the US, and Iran – are well-placed to influence the system for good or ill, should they be moved to do so. They might not be capable of coordinating a 51-percent attack, but we also don't know how the network would cope with the sheer persistence of a large enough minority in the event of a fork.

We also shouldn't forget that modern governments' law enforcement arms remain powerful – think of the power and reach of US anti-racketeering agencies. It's naive technological determinism to assume that a massively decentralized system is impossible to stop, so that (to take one recent claim) the rise of cryptocurrencies will force the end of the War on Drugs.<sup>11</sup> It's just as likely that the FBI will, if need be, open up a War on Bitcoin, which could do it irreparable damage in the legitimate business world. The harm caused by governments' manifest inability to close down the illegal drugs trade has never been a factor in policymaking (outside of Latin America), and bitcoin may become another victim of collateral damage. The founder of bitcoin exchange coin.mx is currently being prosecuted in the US on money laundering charges that could bring a 20-year jail sentence.<sup>24</sup> Anticipation of this, and the hounding of previous cryptocurrency pioneers, is probably why Satoshi Nakamoto has fiercely protected his (or her, or their) anonymity.

Here, I have focused on the currency bitcoin without exploring alternative cryptocurrencies. Neither have I discussed alternative uses of the impressive blockchain idea – for example, to act as a distributed notary and record of contracts. Many of the problems associated with the currency could be adjusted with a few obvious tweaks; for example, if a constant number of altcoins was to be mined in perpetuity (as with Peercoin),<sup>25</sup> then the currency would be inflationary, but not very (and if they were as easily lost as bitcoins, the net effect would probably still be deflationary after enough time passed). It might be possible to build some consumer protection into the system, so that miners wouldn't create coins only for themselves, but also create a few for a central fund to compensate people for losses due to malware.


Given bitcoin's nearly-but-not-quite record in fulfilling the major functions of money, particularly its failure to store value in a predictable way, it could be that the use of the blockchain for other purposes is where its future lies. The blockchain, in essence, uses the resources of a large community to assert and verify a connection between two entities (a wallet and a portion of a bitcoin), while a private key allows a real-world owner of those entities to claim ownership. This structure could revolutionize record keeping, for instance registering land, particularly in places where legal safeguards were limited.

But even then it could also be a means for reducing transparency in business. If the owner is prepared to make his own arrangements for security and backup, then bitcoin has a good claim to preserving anonymity. Would we want this option for land or business ownership, or tax arrangements?

The technology has a future, whether as bitcoin or in another form. It's a brilliant piece of work. But



technology should serve the purpose of humans – not only individuals, but also society as a whole. Decentralization in design and on paper doesn't automatically produce a working system immune to hijacking by motivated groups. Concentrations of power can't be engineered away – the old centers will push back, and new centers will appear.

Digital citizens of good faith need to engage with this fascinating technology, understand its implications, and apply it where it's most needed, without succumbing to the hype. Bitcoin's democratic innovation is that the community prints the authority on the emptiness. We must make sure that the community remains able to withdraw that authority in the future. 


### Acknowledgments

This work is partially supported under SOCIAM: The Theory and Practice of Social Machines, funded by the UK Engineering and Physical Sciences Research Council (EPSRC) under grant number EP/J017728/1.

### References

1. S. Kresge, ed., *The Collected Works of F.A. Hayek Volume 6: Good Money, Part II: The Standard*, Routledge, 1999.
2. K.S. Rogoff, *Costs and Benefits to Phasing out Paper Currency*, working paper no. 20126, Nat'l Bureau of Economic Research, Apr. 2014; [www.nber.org/papers/w20126](http://www.nber.org/papers/w20126).
3. S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, white paper, 2008; <https://bitcoin.org/bitcoin.pdf>.
4. A.M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media, 2014.
5. E. Tymoigne, "The Fair Price of a Bitcoin is Zero," *New Economic Perspectives*, 2 Dec. 2013; <http://neweconomicperspectives.org/2013/12/fair-price-bitcoin-zero.html>.
6. N. Mailer, *The Faith of Graffiti*, Praeger, 1974.
7. G. Lubin, "ROUBINI: 'Bitcoin Is a Ponzi Game and a Conduit for Criminal Activities'," *Business Insider*, 9 Mar. 2014; [www.businessinsider.com/roubini-bitcoin-is-a-ponzi-scheme-and-a-conduit-for-criminal-activities-2014-3?IR=T](http://www.businessinsider.com/roubini-bitcoin-is-a-ponzi-scheme-and-a-conduit-for-criminal-activities-2014-3?IR=T).
8. A. Hern, "Missing: Hard Drive Containing Bitcoins Worth £4m in Newport Land-fill Site," *The Guardian*, 27 Nov. 2013; [www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site](http://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site).
9. J.W. Ratcliff, "Rise of the Zombie Bitcoins," *Let's Talk Bitcoin!*, blog, 22 June 2014; <https://letstalkbitcoin.com/blog/post/rise-of-the-zombie-bitcoins>.
10. T. Hornyak, "One Year Later, We're No Closer to Finding MtGox's Missing Millions Worth of Bitcoins," *PCWorld*, 4 Mar. 2015; [www.pcworld.com/article/2892892/one-year-later-were-no-closer-to-finding-mtgoxs-missing-millions.html](http://www.pcworld.com/article/2892892/one-year-later-were-no-closer-to-finding-mtgoxs-missing-millions.html).
11. D. Frisby, *Bitcoin: The Future of Money?*, Unbound, 2014.
12. Y. Varoufakis, "Bitcoin and the Dangerous Fantasy of 'Apolitical' Money," *Thoughts for the Post-2008 World*, blog, 22 Apr. 2013; <http://yanisvaroufakis.eu/2013/04/22/bitcoin-and-the-dangerous-fantasy-of-apolitical-money>.
13. A. Papapostolou, "Yanis Varoufakis: 'Greece Will Adopt the Bitcoin if Eurogroup Doesn't Give Us a Deal'," *Greek Reporter*, 1 Apr. 2015; <http://greece.greekreporter.com/2015/04/01/yanis-varoufakis-greece-will-adopt-the-bitcoin-if-eurogroup-doesnt-give-us-a-deal>.
14. N. Sardesai, "Who Owns All the Bitcoins – An Infographic of Wealth Distribution," *Cryptocoinsnews*, 21 Mar. 2014; [www.cryptocoinsnews.com/owns-bitcoins-infographic-wealth-distribution](http://www.cryptocoinsnews.com/owns-bitcoins-infographic-wealth-distribution).
15. D. Bradbury, "How Dangerous Is Satoshi Nakamoto?" *CoinDesk*, 23 Nov. 2014; [www.coindesk.com/dangerous-satoshi-nakamoto](http://www.coindesk.com/dangerous-satoshi-nakamoto).
16. "The Magic of Mining," *The Economist*, 10 Jan. 2015; [www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic](http://www.economist.com/news/business/21638124-minting-digital-currency-has-become-big-ruthlessly-competitive-business-magic).
17. D. Goodin, "Infecting DVRs with Bitcoin-Mining Malware Even Easier than You Suspected," *Ars Technica*, 5 May 2014; <http://arstechnica.com/security/2014/05/infecting-dvrs-with-bitcoin-mining-malware-even-easier-you-suspected>.
18. J. D'Herdt, "Detecting Crypto Currency Mining in Corporate Environments," *SANS Institute InfoSec Reading Room*, 26 Jan. 2015; [www.sans.org/reading-room/white-papers/threats/detecting-crypto-currency-mining-corporate-environments-35722](http://www.sans.org/reading-room/white-papers/threats/detecting-crypto-currency-mining-corporate-environments-35722).
19. M. Hearn, "Why Is Bitcoin Forking?" *Medium*, 15 Aug. 2015; <https://medium.com/faith-and-future/why-is-bitcoin-forking-d647312d22c1>.
20. C. Metz, "The Bitcoin Schism Shows the Genius of Open Source," *Wired*, 19 Aug. 2015; [www.wired.com/2015/08/bitcoin-schism-shows-genius-open-source](http://www.wired.com/2015/08/bitcoin-schism-shows-genius-open-source).
21. P. Rizzo, "Ghash.io: We Will Never Launch a 51% Attack against Bitcoin," *CoinDesk*, 16 June 2014; [www.coindesk.com/ghash-io-never-launch-51-attack](http://www.coindesk.com/ghash-io-never-launch-51-attack).
22. E. Mu, "My Life Inside a Remote Chinese Bitcoin Mine," *CoinDesk*, 8 June 2015; [www.coindesk.com/my-life-inside-a-remote-chinese-bitcoin-mine](http://www.coindesk.com/my-life-inside-a-remote-chinese-bitcoin-mine).
23. T. Swanson, "Bitcoins: Made in China," *Bitcoin Magazine*, 12 May 2014; <https://bitcoinmagazine.com/12914/bitcoins-made-in-china/>.
24. Y.B. Perez, "\$100k Bail for Suspected Head of Bitcoin Exchange Coin.mx," *CoinDesk*, 11 Aug. 2015; [www.coindesk.com/100k-bail-for-suspected-head-of-bitcoin-exchange-coin-mx/](http://www.coindesk.com/100k-bail-for-suspected-head-of-bitcoin-exchange-coin-mx/).
25. S. King and S. Nadal, "PPCoin: Peer-to-Peer Cryptocurrency with Proof-of-Stake," white paper, Peercoin, 19 Aug. 2012; <http://peercoin.net/assets/paper/peercoin-paper.pdf>.

**Kieron O'Hara** is a senior lecturer and a principal research fellow in the Web and Internet Science Group in the Electronics and Computer Science Department at the University of Southampton. His research interests include trust, privacy, open data, and Web science. O'Hara has a DPhil in philosophy from the University of Oxford. Contact him at [kmo@ecs.soton.ac.uk](mailto:kmo@ecs.soton.ac.uk).

 Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.