Bulletin of the Atomic Scientists

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rbul20

After the fall: Bitcoin's true legacy may be blockchain technology

Eswar Prasad

To cite this article: Eswar Prasad (2022) After the fall: Bitcoin's true legacy may be blockchain technology, Bulletin of the Atomic Scientists, 78:4, 187-190, DOI: 10.1080/00963402.2022.2087371

To link to this article: https://doi.org/10.1080/00963402.2022.2087371

Published online: 11 Jul 2022.

BULLETIN OF THE ATOMIC SCIENTISTS
2022, VOL. 78, NO. 4, 187–190
https://doi.org/10.1080/00963402.2022.2087371

Routledge
Taylor & Francis Group

After the fall: Bitcoin's true legacy may be blockchain technology

Eswar Prasad

ABSTRACT
Bitcoin and its peers have set off a technological revolution that will transform money, finance, and society. However, the future of cryptocurrencies as financial assets is far from certain – as can be seen from Bitcoin's halving in value in six months since November 2021; the total value of all cryptocurrencies fell from $3 trillion to $1.3 trillion over this period. Rather, it is the underlying technology that enables cryptocurrency – the blockchain – that is likely to prove its true legacy.

KEYWORDS
Bitcoin; blockchain; medium of exchange; financial asset; stablecoins; central bank digital currencies

Bitcoin, the original cryptocurrency, was designed to serve as a medium of exchange that could be used for financial transactions without relying on central bank money or a trusted intermediary, such as a commercial bank or credit card company (Nakamoto 2008). Equally alluring from a libertarian perspective, bitcoin promised to enable transactions using only transacting parties' digital rather than real identities. That is, it enabled pseudonymous transactions. Its creation in 2009, amidst the global financial crisis when trust in governments and traditional financial institutions was at its nadir, perfectly fit the zeitgeist of the time.

How does bitcoin work?

Bitcoin incorporates a variety of technologies and combines them in a clever and innovative manner (Narayanan et al. 2016). Cryptography is used to create secure digital wallets in which users can maintain their bitcoin balances while conducting transactions using publicly identifiable information about those wallets. Another fundamental building block is bitcoin's use of distributed ledger technology – essentially a mechanism for maintaining digital ledgers on multiple computers and keeping them synchronized in real time. Distributed ledger technology contributes to the resiliency of information storage systems because it means that there is no longer a single weak point that can precipitate systemic failure – and any attempts to tamper with one or a handful of computers can easily be detected by other computers on the network.

Despite the term "cryptocurrency" conjuring up visions of information being encrypted, bitcoin is in fact very transparent in most respects. All transactions ever conducted using bitcoin – including timestamps, amounts, and digital identities of the transacting parties – are recorded on public digital ledgers that anyone with an internet connection can easily access.

The validation of transactions on the bitcoin network requires that the nodes (computers) that maintain the digital ledgers accept the transactions as authentic and legitimate. The process of achieving such consensus among the nodes is referred to as Proof of Work, and is executed through a process called mining (Jakobsson and Juels 1999). This involves solving numerical puzzles generated automatically by the bitcoin algorithm. These puzzles can only be solved by brute force computing power – they are not amenable to analytical solutions. The first computer to solve a particular problem gets the privilege of validating a specific block of transactions. The successful miner's reward is in the form of a bitcoin.

Bitcoin mining was initially conducted on regular computers, with the processing power of the devices' central processing units determining the success rate of the miners that used them. It soon turned out that graphics processing units, essentially graphics cards used in higher-end machines, were better suited for the computations needed for cryptocurrency mining.

Much of the mining of bitcoin is now carried out by specialized devices called ASICs, or application-specific integrated circuits. ASICs are tailor-built machines containing computer chips designed with a single, specific purpose. An ASIC can be optimized to mine a cryptocurrency that is based on a specific cryptographic algorithm. Bitcoin ASICs can now be bought for a few thousand dollars, and prospective bitcoin miners are known to buy these by the hundreds or thousands.

Mining pools combine the resources of individual miners. Such pooled resources increase the probability of successful bitcoin mining because the pool, with its

CONTACT Eswar Prasad eswar.prasad@cornell.edu

increased power, has a better chance of being the first to solve the cryptographic problems. Needless to say, it takes a lot of power to run the computers, or clusters of computers, that calculate potential solutions. Moreover, ASICs are run virtually nonstop, causing them to burn out relatively rapidly. Thus, Proof of Work mining has terrible environmental consequences in the form of massive electricity consumption as well as the computer detritus created by the process – consequences whose scale has only gotten worse as bitcoin has risen in value and sparked enormous amounts of mining activity.

Once a block of transactions is validated by a miner, it is chained using computer code to previous blocks of validated transactions. The resulting chain is called the "blockchain" and is an immutable and secure history of the entire transaction record of bitcoin. This approach, pioneered by bitcoin, has spawned a number of other such cryptocurrencies, each of which has its own blockchain that is in effect an electronic ledger maintained on a large number of computers around the world and synchronized in real time, making it tamper-proof and secure.

Despite its destructive fallout, Proof of Work mining is conceptually clever. It also ensures the security of the blockchain as it would take massive amounts of computing power to create a forged copy of the blockchain and get other bitcoin users to accept it as the valid blockchain (which would, in effect, allow bitcoin to be double spent – the digital equivalent of counterfeit banknotes).

Transformation of purpose

For all the conceptual and technical innovations that went into its creation, bitcoin has failed to deliver on its promise as a medium of exchange. It has experienced substantial price fluctuations, from month to month and even from day to day. Its unstable value renders it an ineffective medium of exchange for day-to-day transactions. Moreover, the bitcoin network can directly handle only a small volume of transactions per second and it takes, on average, about 10 minutes for a block of transactions to be processed.

There are other disadvantages to a purported currency that is not issued by a specific institution. Because there is no centralized authority that manages bitcoin, transactions cannot be reversed and mistakes cannot be rectified. Bitcoin balances that are stored in digital wallets can be lost forever if users forget or misplace their passwords (referred to in cryptographic terminology as "private keys").

While it has failed in its stated purpose, bitcoin has become what it was never designed to be – a financial asset. Since bitcoin is a purely digital object without any intrinsic worth, what gives it value?

Bitcoin adherents argue that its scarcity, in addition to its groundbreaking technology, is a fundamental source of its value. The algorithm that controls the creation and use of the cryptocurrency imposes a hard cap of 21 million bitcoins, with about 19 million of those having been created so far. Indeed, advocates have taken to referring to it as digital gold. The underlying logic seems to be that, unlike a fiat currency (one that is issued by a national central bank) such as the US dollar, that can be printed at will and in unlimited quantities by the US Federal Reserve, a scarce object with a steady rate of issuance (one bitcoin is created roughly every 10 minutes) should surely hold its value better.

This is a dubious economic proposition – after all, scarcity by itself cannot be a fundamental and durable source of value. Rather, the sky-high prices of bitcoin and similar cryptocurrencies reflect pure speculative plays, with their value dependent entirely on investors' faith. To a large extent, these prices appear to be predicated on the greater fool theory – all you need to profit from an investment is to find someone who will buy the asset at an even higher price. History is certainly replete with speculative manias that have lasted for a long time and pulled in a large number of investors, but that have usually ended badly (Brunnermeier and Schnabel 2016).

One reason why bitcoin's prices have surged in recent years does in fact have to do with central banks. Like many other central banks, the US Federal Reserve printed enormous quantities of money during and in the aftermath of the global financial crisis of 2008–2009 and also during the brief but sharp COVID-related crisis of 2020. This kept interest rates low and led to a search for yield, with many financial assets, including some risky and highly speculative ones such as bitcoin, benefiting from investor demand and experiencing price increases.

In many troubled economies such as El Salvador (which recently decreed that bitcoin would be legal tender), where the credibility of local currencies has been hurt by economic mismanagement and political instability, bitcoin might be seen as a more reliable alternative despite its high price volatility. It is sometimes used as a way of spiriting savings out of a country rather than leaving money in local currency-denominated bank deposits where the purchasing power of those savings could erode quickly. There are some indications that the demand for bitcoin surged in value when the Turkish lira was plummeting in value.

It is also possible that a number of naïve retail investors have been taken in by the razzle-dazzle of the new technology and poured their savings into crypto assets without fully comprehending the risks. Consequently,

a sharp drop in bitcoin's price could cause a lot of pain even if it doesn't impinge on the broader financial system in the United States or elsewhere.

Beneficial technology

For all its flaws and no matter what happens to its value, bitcoin has set off a revolution that has the potential to generate tangible economic and societal benefits.

Other cryptocurrencies are emerging that overcome many of bitcoin's flaws. For instance, so-called "stablecoins" attempt to fix the problem of unstable value but they do require designated intermediaries to validate transactions. In an interesting irony, stablecoins derive their stable value – a key characteristic for an effective medium of exchange – from their backing by stores of fiat currencies or government bonds, precisely the antithesis of the libertarian underpinnings of bitcoin. A new breed of stablecoins – which were supposed to be backed by reserves of other cryptocurrencies – have proven to be flightier in value. The value of one such stablecoin, TerraUSD, recently plunged by about 90 percent, from $1 to less than 10 cents, in just a few days.

Stablecoins aim to provide low-cost and easily accessible digital payments within and across national borders. This could certainly benefit the poor and the unbanked, as well as small businesses such as street vendors. By reducing the costs and other impediments to international payments, fiat currency-backed stablecoins could benefit international trade and even economic migrants sending remittances back to their home countries.

Equally importantly, the emergence of cryptocurrencies has prodded central banks to start designing digital versions of their own official currencies. Countries such as China, Japan, and Sweden have initiated trials of central bank digital currencies and many others, including Brazil and India, have plans to do so. As a result, cryptocurrencies are indirectly hastening the demise of physical currency.

The blockchain technology that underpins bitcoin is finding uses in other areas of finance. This technology could soon be adapted for a broad range of uses – buying a car or house, managing ownership records for both electronic and physical assets, and maintaining digital registries of public records. Remarkably, such transactions can be executed and recorded on the blockchain through computer algorithms and without the involvement of trusted third parties such as attorneys or bankers. Savers and borrowers could be connected directly, without having to go through banks.

New financial products and services are being built on decentralized blockchains. This bears the promise of democratizing finance by providing widespread access to even basic banking products and services without relying on large and lumbering brick-and-mortar banks. Cryptocurrencies such as Ethereum are more effective at supporting these new financial ecosystems on their blockchains, which could in turn underpin their intrinsic value.

Bitcoin's legacy

The future of bitcoin and such cryptocurrencies as financial assets is murky. Their real value, however, is in catalyzing a revolution that will make low-cost digital payments broadly accessible. New technologies related to cryptocurrencies will help democratize finance by making basic financial products and services easily and widely available to the masses. This will be the true and lasting legacy of bitcoin.

Of course, technology cannot solve all problems and might even create new ones. Financial regulators face particular challenges in updating regulations to cover cryptocurrencies and related financial products to ensure that they do not result in financial instability. Investor protection is a serious concern as naïve retail investors might end up taking on more risk than they realize when they get dazzled by the promise of a quick pathway to riches from the new technologies.

What this potentially disruptive technology means for some of the issues that concern the *Bulletin of the Atomic Scientists* – national security, rogue regimes, nuclear weaponry, and climate change – is still up in the air. Cryptocurrency can be used to help fund the defense of Ukraine, or it can used to fund terrorists while leaving no paper trail. Distributed ledger technology can improve nuclear security, verify the dismantlement of nuclear weapons – or it can lead to a worsening of the climate crisis via environmentally costly bitcoin mining.

Technology by itself is seldom wholly positive or wholly negative. It all comes down to how we humans decide to use it.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

No specific funding for this research, although the author is a member of Cornell's Initiative on Cryptocurrencies and Contracts (IC3), which receives funding from industry partners and foundations.

Notes on contributor

Eswar Prasad is the Nandlal P. Tolani Senior Professor of Trade Policy and Professor of Economics in the Dyson School at Cornell University, a senior fellow at the Brookings Institution, and a research associate at the National Bureau of Economic Research. This article draws on his latest book *The Future of Money: How the Digital Revolution is Transforming Currencies and Finance* (Harvard University Press, September 2021). https://futureofmoneybook.com

References

Brunnermeier, M., and I. Schnabel. 2016. "Bubbles and Central Banks: Historical Perspectives." In *Central Banks at a Crossroads: What Can We Learn from History? (Studies in Macroeconomic History*, edited by M. Bordo, Ø. Eitrheim, M. Flandreau, and J. Qvigstad, 493–562. Cambridge: Cambridge University Press. doi:10.1017/CBO9781316570401.013.

Jakobsson, M., and A. Juels. 1999. "Proofs of Work and Bread Pudding Protocols." In *Secure Information Networks. IFIP — The International Federation for Information Processing*. Vol. 23., edited by B. Preneel, 258–272. Boston, MA: Springer. doi:10.1007/978-0-387-35568-9_18.

Nakamoto, S. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." *White Paper*. https://bitcoin.org/bitcoin.pdf.

Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ: Princeton University Press. https://press.princeton.edu/books/hardcover/9780691171692/bitcoin-and-cryptocurrency-technologies.