Bitcoin: Bauble or Bullion? Bubble or Bulwark for Freedom and Justice?

Kristjan Tomasson

Abstract

The purpose of this paper is to examine in what ways capital-B Bitcoin, the system, and lower-b bitcoin, the unit of account, are or are not money. Bitcoin is the largest, by market capitalization, financial asset labeled "cryptocurrency" and the first decentralized digital currency. The paper canvasses the academic, business and technical literature to scrutinize the validity of this neologism's implied equivalency to money as a concept, system and artifact from historical, economic, political, teleological, theoretical and functional perspectives. The author(s) of Bitcoin invented blockchain, that is a shared, decentralized, time stamped, public ledger, to solve the problem of double spending. The risk of fraud, paying several counterparties with the same coin, was an intractable limitation on digital cash replacing paper money. The addition of blockchain to "proof of work" and advanced cryptography was a major advance in electronic cash systems. The combination of other features with this innovation, in particular a programmed steady growth and overall limit on supply, created in Bitcoin and other cryptocurrencies that followed a potential challenger to fiat currencies. This paper tests Bitcoin's progress and prospects in credibly replacing sovereign currencies in theory and in practice. Our conclusion is that the replacement of fiat currencies by cryptocurrencies in the world economy is not imminent. However, the underlying technology of cryptocurrencies holds great promise for improving the security and efficiency of the global financial and monetary systems.

Introduction

"The process by which money is created is so simple that the mind is repelled."

John Kenneth Galbraith, *Money: Whence It Came, Where It Went*

Economist and money historian, John Kenneth Galbraith, did not live to witness the advent of bitcoins.[1] If he had, he could have ably illuminated the debate on whether bitcoin is money and if the Bitcoin system legitimizes money creation. It took an unusually long time, over a quarter of a century, until advances in cryptography made digital money possible and a practical application of the technology came to fruition.[2] Digital currencies had their foundation in the early 1980s when David Chaum

1 This paper will follow the convention in the computer science literature of using capital-B Bitcoin to refer to the system and the lower-b bitcoin to refer to the unit of account.

2 Tschorsch, Florian and Björm Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," IEEE Communications Surveys & Tutorials, 18, no.3

published his seminal "Blind Signatures for Untraceable Payments" on using advances in cryptology to devise a virtual currency.[3] His conception of a digital payment medium relied on a trusted third party, typically a financial institution, as did the many virtual currencies that followed until Bitcoin was invented. Money is a building block of human society that has facilitated and increased human exchanges beyond barter. It constitutes a cornerstone of the economy, the financial and monetary systems, and society itself.

Where did Bitcoin (and bitcoins) come from? What are they?

Bitcoin was launched publicly as a whitepaper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System*, posted online on October 31, 2008 by the unknown author(s) Satoshi Nakamoto.[4] The financial crisis of 2007-08 was, in the view of many economists, the worst financial crisis since the Great Depression of the 1930s. By the time Nakamoto posted the foundational document for Bitcoin, the financial crisis of 2007-08 was full-blown and had spread globally. The bankruptcy of Lehman Brothers on September 15, 2008 was the largest in history. With assets of $639 billion and 25,000 employees, Lehman was the fourth-largest investment bank in the United States at the time.[5] Equity markets around the world lost nearly $10 trillion in market capitalization in October of 2008. Confidence in the financial system was shaken to its core. It hardly seems coincidental that Bitcoin, a currency that sidestepped the need for trust in financial institutions, emerged during the financial crisis of 2007-08.

The Internet made possible commercial transactions of all sorts between businesses and individuals without the need for physical proximity. Until the advent of Bitcoin, this was true in all respects except payment – especially the equivalent of cash payment. Cryptographic protocols to create electronic signatures quickly emerged as the necessary building block for a digital currency to fill this need of the Internet marketplace. Notably, several digital currencies, aimed at providing security and efficiency to online payments, preceded Bitcoin. Hal Finney created the concept of "proof of work," which was later added to advanced cryptography in the digital currency schemes of Nick Szabo (bit gold) and Wei Dai (b-money).[6] Digital signatures provide "strong control of ownership, but...not a means to prevent double spending."[7] A major challenge for early digital currencies was the possibility of double spending - transferring the same coin

(March 2, 2016), 2084-2123.

3 Chaum, David, "Blind Signatures for Untraceable Payments," CRYPTO '82: Proceedings of the 2nd Conference on Advances in Cryptology (1982), 199–203.

4 Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System* (October 31, 2008) https://bitcoin.org/bitcoin.pdf

5 "The collapse of Lehman Brothers: A case study" (Updated December 11, 2017 — 3:07 PM EST) https://www.investopedia.com/articles/economics/09/lehman-brothers-collapse.asp

6 Dai, Wei, "Wei_Dai comments on AALWA: Ask any Less Wronger anything," *Less Wrong, A community blog devoted to refining the art of human rationality,* (January 12, 2014) http://lesswrong.com/lw/jgz/aalwa_ask_any_lesswronger_anything/ap3c

7 Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 8.

to different recipients. Even with a reliably confirmed digital signature, a trusted third party, such as a financial institution, had to be interposed between online payor and payee to execute payment using a cryptocurrency. The necessity of a trusted third party, however, created transaction costs that were inefficient to the point that handling small payments, a primary function of cash, was uneconomic. Furthermore, "since financial institutions cannot avoid mediating disputes...the cost of mediation...[results] in the loss of ability to make non-reversible payments for non-reversible services."[8] Bitcoin offers an effective solution to the problem of someone being able to spend the same token twice; it also successfully deals with other types of fraud possible in electronic payments. Bitcoin's replacement for the trusted third party is the blockchain, essentially a shared, decentralized, timestamped public ledger.

The ledger is a database that holds the complete history of every transfer of every bitcoin ever "mined" and circulated, in incorruptible chronological order. It is distributed throughout a peer-to-peer network of computer "nodes," that is, pools of thousands of computers, around the world. The network is open, "nodes can leave and rejoin the network at will," and access to the ledger is public. A transfer of a bitcoin is a transaction validated by timestamp, verified based on "proof of work." The "work" consists of the nodes of computers in the network competing to solve massive mathematical trial-and-error puzzles using the encrypted code or "hash" of transactions. The hash of each transfer is matched against the published history of all transactions. Once a solution is found, it is checked by the other nodes, and verification is achieved once a majority of nodes agree on the solution – which then adds a block to the chain. Solving the puzzles requires utilizing massive computing power and energy. As incentive to invest capital and electricity, nodes are rewarded with bitcoins for being the first to solve a puzzle. The process was designed to be "analogous to gold miners expending resources to add gold to circulation." In the case of bitcoin creation, it is "CPU time and electricity that is expended."[9] This is why the bitcoin-creation process is referred to as "mining" and the nodes as "miners." Bitcoin, then, not only "cleverly combines existing contributions from decades of research, but also solves fundamental problems in a highly sophisticated, original and practically viable way: it uses a proof of work scheme to limit the number of votes per entity, and thus renders decentralization practical."[10]

The security of the network is robust due to its "unstructured simplicity." Both the rules of the network itself and the mining process are governed by majority, based on the doctrine of "one-CPU-one-vote." The competition among nodes keeps power over the currency diffused. The window of opportunity to attack the network and falsify results is so time-restricted that it becomes "computationally impractical."

Advances in cryptography and computing speeds were among the crucial developments in science and technology that made Bitcoin realizable. Timothy C. May, perhaps better

8 Ibid, 1.

9 Ibid, 4.

10 Tschorsch, Florian and Björn Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," 2084.

known as a founding member of the "Cypherpunks mailing list,"[11] wrote "The Crypto Anarchist Manifesto."[12] In it, he predicts a social and economic revolution caused by:

> the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive rerouting of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.[13]

This manifesto lays out a political agenda that inspired many contributors to the evolution of cryptocurrencies.

What is money?

Money is commonly defined by three basic functions it performs, as a: medium of exchange, store of value, and unit of account. These basic economic functions are what make money an integral component of a free market economy. Georg Simmel, the renowned neo-Kantian sociologist, analyzes money as both an economic and a social institution, which traces its roots back to the foundations of civil society. Before there

11 Cypherpunk is a pun on "cyberpunk." "Cyberpunk" refers to the subculture that evolved in the1990s when computers and networks were added to "punk," a movement about resistance to authority and convention "heavy on fashion and light on politics...aesthetic anarchy," originating in the 1980s and '90s. "The 1990s were a time of extraordinary hope...The end of the Cold War and the peaceful collapse of the Soviet Union released an intoxicating sense of optimism, at least in the West. Washington debated the "end of history," with liberal market economies coming out triumphant. In the Persian Gulf War of 1991, perhaps America's shortest and most successful ground war operation to date, the Pentagon overcame the mighty Iraqi army — and with it the lingering Vietnam hangover. Silicon Valley and America's technology startup scene, still bathing in the crisp utopian afterglow of the 1980s, watched the rise of the New Economy, with vertigo-inducing growth rates. Entrepreneurs rubbed their hands in anticipation. Intellectuals were inebriated by the simultaneous emergence of two revolutionary forces: personal computers and the internet. More and more PC owners connected their machines to the fast-growing global computer network, first with clunky, screeching modems, then with faster and faster broadband connections.

12 May, Timothy C. "The Crypto Anarchist Manifesto" (November 22, 1992). https://www.activism.net/cypherpunk/crypto-anarchy.html/

13 Ibid.

could or needed to be money, there had to be exchange. And, exchange came into existence simultaneously with and as a part of society:

> the exchange of the products of labour, or of any other possessions, is obviously one of the purest and most primitive forms of human socialization; not in the sense that 'society' already existed and then brought about acts of exchange but, on the contrary, that exchange is one of the functions that creates an inner bond between men—a society, in place of a mere collection of individuals.[14]

Digital networks, the most prominent being the Internet, have expanded the opportunities for human exchange exponentially, and, therefore, have made possible the circumscription of myriad overlapping affinity groups of any size. Applying Simmel's teleological insight, we can see that a digital currency is a necessary element to make a cyber network a society.

Ludwig von Mises developed the "regression theorem," building on Carl Menger's Principles to determine the purchasing power of money. It is both a theoretical and historical explanation of the evolution of money. The purchasing power of money is based on the market:

> track[ing] [it] back step by step, we finally arrive at the point at which the service of the good concerned as a medium of exchange begins. At this point yesterday's exchange value is exclusively determined by the nonmonetary – industrial – demand which is displayed only by those who want to use this good for other employments than that of a medium of exchange.[15]

The Austrian School of revived classical economics, thus, advocates for a return to "sound money." They believe strictly in commodity money, specifically the gold standard as "what it meant in the nineteenth century."[16] In the neoclassical prescription, the combination of a commodity standard for the currency and constraints on fractional reserve banking limit governments' ability to manipulate the money supply and interest rates. Ludwig von Mises remarked that "inflation is the true opium of the people administered to them by anti-capitalist governments and parties." According

to the Austrian school of thought, political management of the money supply distorts capital allocations and can create catastrophic imbalances.[17]

14 Simmel, Georg, *The Philosophy of Money*, 3rd ed., ed. and trans. David Frisby (London: Routledge, 2004), 174.

15 von Mises, Ludwig, "Part Four: Catallactics or Economics of the Market Society, Chapter XVII. Indirect Exchange," in *Human Action* (1940), 778.

16 von Mises, Ludwig, "Part Four: Monetary Reconstruction, Chapter III The Return to Sound Money, § 2 The Integral Gold Standard," in *The Theory of Money and Credit* (New Haven: Yale University Press, 1953), 438. https://mises.org/system/tdf/The%20Theory%20of%20Money%20and%20Credit_3.pdf?file=1&type=document/

17 Ibid, 442.

In contrast, Keynesian theory holds that monetary and fiscal policies are crucial tools to manage the economy. The central bank can stimulate short-term demand by increasing the money supply, thereby lowering interest rates. Under this theory, governments can smooth out business cycles and help pull an economy out of a recession.

The state stepped into the role of trusted third party to legitimize money early on in the development of currency and charged seigniorage in exchange. Initially, when currency was primarily in the form of metal coins, seigniorage was ostensibly a tax reflecting the costs to acquire that metal, mint the coins, and distribute them. For paper money, seigniorage includes production and distribution costs, as well as interest, which can be a cost addition or subtraction depending on whether the central bank purchases (creates new money) or sells (issues bonds or notes) securities. An increase of the money supply shifts purchasing power away from holders of the currency to the issuing government. This devaluation of the currency is what economists sometimes label as "inflation tax." To the extent that a private cryptocurrency can compete with fiat currencies, it offers the possibility of removing governments' ability to seize purchasing power without conspicuous taxation. The Austrian and Keynesian schools differ sharply on whether the abrogation of governmental monetary intervention would be a benefit or a detriment to the economic and political systems.

Is Bitcoin money - a real currency?

Nowhere in the foundational document, Bitcoin: A Peer-to-Peer Electronic Cash System, do the author or authors refer to Bitcoin as a currency, nor do they call it money directly. Satoshi Nakamoto was seemingly concerned only with creating a reliable and efficient electronic payment system by solving the "double-spending" problem, without the cost of a financial institution as the trusted intermediary. If the inventor(s) considered the broader economic and political consequences of the decentralized nature of their payment system, they did not address them in the whitepaper. Let us examine in what ways Bitcoin could be qualified as a currency that could compete with, or, as some proponents insist, even replace the fiat currencies that constitute the global monetary system today.

As of 2015, bitcoin was accepted as a medium of exchange (i.e. for payment) by over 160,000 merchants including several big names such as Expedia, Microsoft, and Dell. This universe of counterparties, however, is still small in the context of the economy. Bitcoin was designed to reduce transaction costs, which ought to make it attractive as a medium of exchange especially for microtransactions. The biggest jump in the number of merchants taking payment in bitcoin occurred after some major payment platforms – namely, PayPal – adopted bitcoin. This is ironic because it eliminates, to the detriment of consumers, the cost advantage of bitcoin as payment.[18] There are several problems with bitcoin as a currency that have come to light since its deployment in the market.

18 "What Can You Buy with Bitcoin?" *Coindesk.com* (October 19, 2015). http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/

Most importantly, bitcoin's value has exhibited high volatility and low correlation against all the major world currencies and gold. Volatility of the bitcoin-U.S. dollar exchange rate was 142% in 2013, compared to a volatility range of 7-12% for the U.S. dollar against the euro, yen, British pound, and Swiss franc, and 22% versus the price of gold. As reference, even highly speculative stocks seldom reach 100% volatility, and broadly held stocks tend to exhibit volatilities between 20% and 30%.[19] Bitcoin's extreme volatility most impairs its utility as a store of value.

In 2013, the prices of the major fiat currencies and gold were all strongly, positively correlated with each other – particularly the European currencies, with a correlation ranging from 0.42 to 0.64. During this same year, there was a negligible (ranging from -0.06 to 0.01) correlation between the bitcoin-U.S. dollar exchange rate and any of the leading currencies and gold. These results imply that the macroeconomic and geopolitical events that influence the relative prices of the major world currencies and gold have little-to-no impact on the value of bitcoin.[20] A commodity trading strategist for RBC pointed to the possible emergence of an increased correlation between bitcoin and gold in late 2017 and early 2018.[21] It is still early in the life cycle of bitcoin, and all of its market characteristics are changing rapidly. More history and data are needed before we can establish whether bitcoin is a currency or a commodity, in terms of its price behavior.

Bitcoin's market capitalization grew from $1.3 billion at the beginning of May 2013 to $23.9 billion four years later – a pace that seemed extraordinarily rapid in terms of any historic comparison. The market capitalization then spiked to peak at $318.3 billion on December 18, 2017, over a thirteenfold increase in less than 8 months. It has since fallen back down to around $134 billion as of mid-March 2018. The 24-hour trading volume in bitcoin did not reach $100 million until December 2016 and peaked at $23.4 billion at the start of 2018. As of the ides of March 2018, trading volume is in the $5-10 billion range daily.[22]

Precedent set by other asset classes would suggest that bitcoin's volatility would decline as its market capitalization grows. A 2013 study by the National Bureau of Economic Research looked for individual U.S. stocks with sufficient correlation to serve as a hedge for bitcoin via short selling. The closest proxy they could find was Vitamin Shoppe, a public specialty retail company with a $2 billion market capitalization, which could

19 Yermack, David, "Is Bitcoin a Real Currency? An Economic Appraisal," *NBER (National Bureau of Economic Research)* Working Paper 19747 (December 2013), 14-15. http://www.nber.org/papers/w19747/

20 Ibid, 15.

21 Shen, Lucinda, "Forget the Stock Market. Investors Are Trading in Gold for Bitcoin," *Fortune* (February 8, 2018). http://fortune.com/2018/02/08/bitcoin-price-cryptocurrency-gold-price-buy/

22 "Cryptocurrency Market Capitalizations: BTC," coinmarketcap, (March 17, 2018). https://coinmarketcap.com/currencies/bitcoin/

not serve a hedging function for cryptocurrencies on any impactful scale.[23] Bitcoin volatility declined substantially starting in 2014 and picked up relatively modestly in the second half of 2017 through the middle of March 2018. In July of 2017, the U.S. Commodity Futures Commission granted the first license to clear and settle derivative contracts for digital currencies to LedgerX, a New York-based exchange and clearing house.[24] By the end of 2017, several market participants around the world had launched cryptocurrency-related derivatives. In January of 2018, European financial regulators revealed that they were evaluating the prospect of including limits on cryptocurrency derivatives in their broader crackdown on leveraged trading platforms.[25] U.S. regulators are taking a more laissez-faire approach, the CFTC allows self-certification by exchanges to be able to bring products to market faster.[26] The massive growth of the market capitalization of bitcoin, the emergence of hedging products and the early suggestions of a trend towards lower volatility all indicate that cryptocurrencies are maturing as an asset class. For institutional investors, cryptocurrencies are becoming too large to ignore as a potential investment and diversification vehicle, whether they are currency, commodity or something else.

High price volatility makes it unattractive for merchants to accept bitcoins. The currency can lose value greater than credit card fees (typically 2-3%) faster than it can be converted to fiat currency. Most merchants convert bitcoins to fiat currency immediately and do not carry any bitcoin inventory, which makes for another complication - returns. Since bitcoin transactions are irreversible, merchants typically offer in-store credit denominated in fiat currency.

Clearing delays for bitcoin payments have climbed to 10 minutes or more – and can be up to an hour – which pose serious technical problems for the transactional efficiency of the currency.[27] This is due to block size limits set in the underlying structure of the Bitcoin blockchain, which increase risk and reduce liquidity to the point of impracticality. New companies have emerged that offer to insure the risk of double payment during the clearing delay, but this service adds a 0.1% fee to the transaction. The limit imposed by block size is a flaw that seriously constrains bitcoin's long-term potential as a currency.

---

23 Yermack, "Is Bitcoin a Real Currency? An Economic Appraisal," 15-16.

24 Chavez-Dreyfuss, Gertrude, "LedgerX Gets U.S. Approval for Derivatives on Digital Currencies." *U.S. Reuters,* (July 24, 2017). https://www.reuters.com/article/us-usa-cftc-digitalcurrency/ledgerx-gets-u-s-approval-for-derivatives-on-digital-currencies-idUSKBN1A92FZ

25 Murphy, Hannah, "Regulators eye ban on cryptocurrency derivatives bitcoin," *The Financial Times* (January 18, 2018). https://www.ft.com/content/d6df33a0-fc4e-11e7-9b32-d7d59aace167

26 Meyer, Gregory, "US derivatives regulator looks to calm cryptocurrency fears," *The Financial Times* (January 31, 2018). https://www.ft.com/content/db9d547e-06b4-11e8-9650-9c0ad2d7c5b5

27 Böhme, Rainer, et al., "Bitcoin: Economics, Technology, and Governance," *The Journal of Economic Perspectives* 29, no. 2 (Spring 2015), 217.

When Bitcoin was launched, a bitcoin could be mined on an average personal computer in a few hours. Today, it would take that same computer over a century to mine just one bitcoin. Mining takes ever-increasing investment in computing power, because the network increases the difficulty of the mathematical problems to keep the production of bitcoins at the constant rate set in the design, as the number of miners competing rises.[28] Therefore, individuals who want to acquire a non-negligible quantity of bitcoin typically must purchase them from exchanges with fiat currencies.

The exchange system has created security risks and pricing inefficiencies for Bitcoin. First, it introduces an external process reliant on third parties to enter the Bitcoin economy. Further, while Bitcoin itself may be virtually unhackable, the exchanges and other third-party service providers are vulnerable to both hacking and more traditional "analog" fraud. The very first exchange, Mt. Gox, which, at its peak, was handling 70% of all bitcoin transactions, went bankrupt in 2014. Mt. Gox customers lost 850,000 BTC (BTC is a commonly used abbreviation for bitcoin, the currency; however, the still unofficial ISO 4217 currency code for bitcoin is XBT), equivalent to $480 million at the time, to hackers with no recourse or insurance for their lost tokens. This caused the price of bitcoins to decline for more than a year.[29]

Substantial disparities, as high as 14%, in prices of bitcoins among different exchanges came to the forefront, in the build up to the Mt. Gox bankruptcy and the proliferation of exchanges that gained market share in its wake.[30] These value discrepancies ostensibly reflect the variability in the perceived risk of different exchanges as counterparties for buyers of bitcoins. Price discrimination is present in the other direction as well. Bitcoins are embedded with a complete and permanent history of transactions and some bitcoins have been stolen or used in illicit trades (e.g. drugs, gambling, arms dealing, money laundering). Even though the system is designed to be anonymous, the reputations of some specific bitcoins and some owners of bitcoins are sullied in the marketplace; bitcoins identified as dirty are sometimes either not accepted or priced lower by exchanges and other counterparties. These factors challenge bitcoins' fungibility and thereby their utilitarian value as a currency.[31]

Bitcoins have grown in value from 4.951 cents at inception to a high of nearly $20,000.00 per token as recently as a few months ago. As of mid-March 2018, one bitcoin is trading in the $8000-$9000 range. The high unit value poses a problem opposite to that faced by Germany during the hyperinflationary period of the 1920s, when emergency money

28 Beigel, Ofir, "Is Bitcoin Mining Profitable in 2017?" *99 Bitcoins* (March 8, 2017). https://99bitcoins.com/bitcoin-mining-profitable-beginners-explanation/

29 Popper, Nathaniel, "Mt. Gox Creditors Seek Trillions Where There Are Only Millions," *The New York Times* (May 25, 2016). https://www.nytimes.com/2016/05/26/business/dealbook/mt-gox-creditors-seek-trillions-where-there-are-only-millions.html?_r=0

30 Bitcoin beta, https://bitcoin.stackexchange.com/questions/12670/why-dont-people-buy-at-one-exchange-and-sell-at-another

31 Vorick, David, "Ensuring Bitcoin Fungibility in 2017 (And Beyond)," *Coindesk.com* (December 28, 2016). http://www.coindesk.com/ensuring-bitcoin-fungibility-in-2017-and-beyond/

was created to accommodate the high denominations of everyday retail transactions. Today, prices for common goods (i.e. anything under $15), when expressed in bitcoin, require three or more decimal places before reaching the first decimal point greater than zero. This seemingly minor characteristic makes bitcoin unwieldy as a unit of account. According to research on spending and consumption behavior, the denomination effect would suggest that most consumers are not as fluent evaluating or comparing the price of, say, a loaf of bread at 0.000464 BTC as they would be at $3.99.[32] Furthermore, many common financial accounting software programs are designed to handle only two decimal points. This problem could be resolved by simply using smaller units such as milli- or micro bitcoins. However, such a change has not been implemented to date, even though there is ample marketing research to suggest that consumers are turned off by difficult calculations for price comparisons.[33] The clumsiness of the large unit size is likely not an insignificant reason that bitcoins have yet to be accepted widely as a unit of account and a medium of exchange.[34]

In addition to defining how bitcoins are created through mining, the Bitcoin algorithm prescribes the schedule of production of bitcoins. It sets the maximum total supply of bitcoins, an asymptote, at 21 million, due to a technical limitation in the data structure of the blockchain. The rate of growth in computing speeds determines the actual schedule of production of bitcoins. Current estimates yield a projected date for the last bitcoin to be mined around the year 2140.[35] Inevitably, some bitcoins will be lost (e.g. the private key necessary to spend a given bitcoin may be lost by its owner), destroyed (i.e. willfully sent to an address where they get stuck as impossible to spend), or become un-spendable owing to "technical peculiarities" (known to date, there are three such transactions, worth 50 BTC each, where technical peculiarities resulted in un-spendable coins).[36] The spendable supply of bitcoins will, therefore, be somewhat smaller than the theoretical maximum number of 21 million bitcoins.[37] Fiat and gold-based currencies are controlled and tracked by a centralized government authority; in those monetary systems, central banks and fractional reserve banking can increase the supply of money according to the government's political and economic agendas. The inflation tax is seen as an unjust redistribution of purchasing power by libertarians and anarchists. The wholly decentralized nature of Bitcoin, especially the scheduled growth and finite supply of bitcoins, is one of the features that appeals most to proponents of the currency.

In certain ways, bitcoin's characteristics parallel those of the major currencies that were pegged to a gold standard in the 19th and early 20th centuries. Bitcoin's transparent and

32 Koschate-Fischer, N. & Wüllner, K. *Journal of Business Economics* (2017) 87: 809. https://doi.org/10.1007/s11573-016-0839-z

33 Ibid.

34 Yermack, "Is Bitcoin a Real Currency? An Economic Appraisal," 12-13.

35 Ibid, 4-5.

36 "Controlled Supply" https://en.bitcoin.it/wiki/Controlled_supply#Technical_peculiarities_preventing_spending_of_bitcoin Accessed May 1, 2017.

37 Ibid.

finite growth eliminates the ability of governments to manipulate the economy through the money supply and interest rates. Despite this, most Austrian School economists reject the notion that bitcoin could replace fiat currencies, chiefly on the basis that its value is not derived from a commodity. Some Austrian School adherents, notably Konrad Graf, disagree with this analysis and argue that bitcoin "had some antecedent value...as [for example] a geek toy, as art, or as social marker."[38] Graf further argues that bitcoin is a scarce, intangible digital good that meets the criteria of being a commodity under von Mises's regression theorem.

The velocity of circulation of bitcoins suggests that a majority of bitcoin holders bought their bitcoin for speculative purposes, as they do not spend them. In one study of blockchain data spanning from 2009 to 2012, Dorit Ron and Adi Shamir found that only about half of the bitcoins purchased were spent in the first three months after acquisition.[39] These findings are consistent with the relatively few number of merchants that accept bitcoin. This is evidence that the Keynesian "transaction motive" is underrepresented in creating demand for bitcoin. Therefore, it is not useful in stimulating short-term aggregate demand in the economy. Bitcoin's decentralized nature eliminates the important Keynesian tool of monetary policy. Keynesian economists have neither devoted much attention to Bitcoin nor reached a consensus view. Nobel laureate and Keynesian economist, Paul Krugman, wrote a blog entitled "Bitcoin Is Evil" that received much attention. In it, he questions bitcoins' reliability, primarily as a store of value but also as a medium of exchange.[40]

The growth in the market capitalization of bitcoin is remarkable for both its size and speed. So far, however, bitcoins only partially perform the basic functions of a true currency. The biggest obstacle across all three money functions is its price volatility, which is extreme for any financial asset, let alone for cash. This volatility is exacerbated by the speculative motives of most of its holders. Bitcoin's utility as a medium of exchange is further limited by: the comparatively small universe of merchants that accept it; the counterproductive addition of fees like those credit cards incur; mounting clearing delays; and the laboriousness of procuring the coins. The cryptocurrency's price instability is its major weakness as a store of value, but that role is further challenged by its nearly total absence of correlation with macroeconomic and geopolitical events. Its usefulness as a unit of account is also hindered by the clumsiness of its unit size, which makes price comparisons and accounting cumbersome. Because bitcoin's value is not tied to a commodity, it is not a theoretical fit as a valid currency according to neoclassical economics. Its disinflationary, finite, and constantly growing supply renders

38 Peter St. Onge, "Cryptocurrencies and a Wider Regression Theorem," Mises Institute (December 11, 2014). https://mises.org/library/cryptocurrencies-and-wider-regression-theorem/

39 Ron, Dorit and Adi Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," in: Sadeghi AR. (eds) *Financial Cryptography and Data Security.* FC 2013. Lecture Notes in Computer Science, vol 7859 (2013).

40 Krugman, Paul "Bitcoin Is Evil," *The New York Times* (December 28, 2013). https://krugman.blogs.nytimes.com/?s=bitcoin/

it independent of government intervention and therefore objectionable to Keynesians, were it to replace fiat currency to a significant degree. As for its political and social functionality, Bitcoin falls somewhat short as well. Its theoretical anonymity (heuristics can easily breach the privacy of transactions) serves a libertarian and anarchist agenda by providing and protecting certain freedoms but to an incomplete degree.

Was Bitcoin intended to be a real currency?

The inventor(s) did not discuss either how they perceived or intended Bitcoin to fit into the monetary system or the broader political economy. The infamous Satoshi Nakamoto's true identity remains undiscovered. However, among the many antecedent cryptocurrencies, Bitcoin's heritage has been linked, in particular, to bit gold invented by Nick Szabo, and b-money created by Wei Dai. This is because they were the first to add reusable proof of work (RPOW) to digital signatures, based on advanced cryptography in digital cash. RPOW was developed by fellow Cypherpunk, Hal Finney, the recipient of the very first bitcoin from Satoshi Nakamoto.[41] The Cypherpunks are rooted in cryptoanarchism, a movement that came out following the invention and spread of public-key cryptography. Its implementation was made possible by the democratization of computing power. Advanced cryptology enabled real anonymity, total privacy, at lightning speed across the globe.

Nick Szabo, a computer scientist and law school graduate specializing in cryptography, thought and wrote about regulation and enforcement of financial transactions on the Internet before he imagined bit gold. In 1997, he published a paper on "smart contracts" that "combine protocols with user interfaces to formalize and secure relationships over computer networks."[42] This concept has since been successfully implemented. For example, auto lenders use GPS to track and, when necessary, seize their collateral by remotely disabling the car's ignition.[43] When Szabo laid out his concept for bit gold on his blog, Unenumerated, he expanded the context of cyberanarchy beyond its anarchic, "libertarian" focus on freedom from government scrutiny, control, and taxation. He identified that dependency on "trust in a third party" (i.e. governments) for the value of "our money," presumably fiat currencies, has led to disastrous "inflationary and hyperinflationary episodes during the 20th century." He observed that "all [the] money mankind has ever used has been insecure in one way or another...from counterfeiting to theft...the most pernicious of which has probably been inflation."[44]

41 Southurst, Jon, "Hal Finney Passes Away," *Coindesk.com* (August 29, 2014). http://www.coindesk.com/bitcoin-pioneer-hal-finney-passes-away/

42 Szabo, Nick, "Formalizing and Securing Relationships on Public Networks," *first monday, Peer Reviewed Journal On The Internet*, 2, no. 9 (September 1, 1997). http://firstmonday.org/ojs/index.php/fm/article/view/548/469#Conclusion

43 Ferro, Shane, "The alleged Bitcoin founder went to law school for fun — and that says a lot about what Bitcoin is really for," *Business Insider* (May 15, 2015). http://www.businessinsider.com/bitcoin-is-about-property-law-2015-5/

44 Szabo, Nick, "Bit gold," Unenumerated, An unending variety of topics (December 27, 2008)

Wei Dai, in his 1998 proposal for b-money, was narrowly focused on developing a protocol to serve as a "medium of exchange (money) and a way to enforce contracts" without the intermediation and enforcement services of "government or government sponsored institutions."[45] He also specified that he wanted to provide these services to all comers, including illegal entities. The aim of Dai's protocol was to make possible a crypto-anarchic community by enabling "efficient cooperation among its participants."[46] The impetus for Dai's invention was his "fascination" with Tim May's definition of crypto-anarchy. Dai understands May's vision as differentiated from traditional anarchy, because:

> in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.[47]

It seems Dai wants to help create a society that is equally as radical as "traditional" anarchy advocates for, with "government...permanently forbidden." However, his form of anarchy is more pacifist, as government would be rendered "permanently unnecessary" because "violence [becomes] impossible" thanks to absolute anonymity in all b-money transactions.

In an interview Dai gave in 2014, responding to questions about Satoshi Nakamoto's anarchist motivations, Dai opined that Nakamoto likely doesn't consider himself a crypto-anarchist. Dai suggests that Nakamoto "might have been motivated more by a distrust of financial institutions and government monetary authorities and wanted to create a monetary system that didn't have to depend on such trust."[48] Dai thereby confirms that his own intent with b-money was crypto-anarchic in a broader, more radical sense. However, he never provides details on how the impossibility of violence in contractual financial transactions, because of absolute anonymity, translates to a purely pacifist community. Georg Simmel did identify "that exchange is one of the functions that creates an inner bond between men—a society, in place of a mere collection of individuals."[49] Exchange is thus seminal, insofar as it is a necessary, but insufficient, condition to create society.

Another crypto-anarchist, Julian Assange, illuminates the power of anonymity in his introduction of himself as the main researcher for Underground, Suelette Dreyfus's book on early computer hackers. He opens with an Oscar Wilde quote: "Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth."[50] This observation highlights an inherent contradiction in the constitution

45 Dai, Wei, "B-Money," (1988). http://www.weidai.com/bmoney.txt

46 Ibid.

47 Ibid.

48 Dai, Wei, "Wei_Dai comments on AALWA: Ask any Less Wronger anything - Less Wrong."

49 Simmel, *The Philosophy of Money*, 174.

50 Manne, Robert, "The Cypherpunk Revolutionary," *The Monthly* (March, 2011). https://

of Bitcoin. Privacy is a central feature of Bitcoin as an "electronic cash system," and is indeed effective at protecting participants in the Bitcoin economy from violence. A counterparty in a financial transaction cleared through Bitcoin can rely on the unhackability of the system for straightforward enforcement of the terms of any commercial agreement. Furthermore, because the parties to the transaction remain unknown to each other and the world, no one can target anyone else for theft, or any extra-legal enforcement of some grievance, based on knowing where the bitcoins lie. On the other hand, anonymity neutralizes Bitcoin's effectiveness as a society-building medium of exchange considering Georg Simmel's insight.

The foundational document of Bitcoin gives no clear hint as to the underlying political agenda, despite the apparent received heritage of its more political but mixed antecedents. The open and persistently pseudonymous posting of the Bitcoin protocol can be interpreted several ways. It results in no profits or royalties for the inventor(s), which may be a sign of cryptoanarchist sentiments. It may also be a simple fear that with ownership responsibility might come legal prosecution. No thought seems to have been given to the negative social impact of anonymity, which could be seen as technocratic indifference. The evidence suggests that Bitcoin was simply a clever and original technological advancement motivated by practicality over politics.

Bitcoin's future

There are signs of progress in Bitcoin's quest for legitimacy as money. Magistrate Judge Amos Mazzant of the Eastern District of Texas ruled in 2013:

> it is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and as Shavers [the defendant accused of being the 'Bernie Madoff' of Bitcoin for allegedly running a Ponzi scheme through his Bitcoin Savings & Trust, robbing investors of Bitcoin worth $4.5 million at the time] stated, used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the U.S. dollar, euro, yen, and yuan. Therefore, Bitcoin is a currency or form of money, and investors wishing to invest in BTCST provided an investment of money.[51]

The ruling conferred legal status to the definition of bitcoin as money. Ironically, the case also exposed vulnerability in Bitcoin security, even though it was extraneous to Bitcoin's nature and structure.

www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary/

51 Hill, Kashmir, "Federal Judge Rules Bitcoin Is Real Money," *Forbes* (August 7, 2013). https://www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-bitcoin-is-real-money/#1acf9a8a27b8/

There have been some headwinds as well. The Winklevoss twins sank a large portion of the settlement for their role in founding Facebook into bitcoins and related projects, including a bitcoin ETF. They filed for SEC approval of the prospectus for the fund, which would have been available to individuals and institutions large and small. The SEC rejected the application on March 10 of 2017, citing that there are no regulated exchanges for bitcoin. The SEC also turned down a second ETF seven days later. While these are setbacks for the recognition of Bitcoin, the mere fact that serious sponsors are investing time and expenses into trying to establish SEC-regulated vehicles for investment in bitcoins is a bullish sign for bitcoin legitimacy.[52]

More promising than bitcoin's future as a replacement for fiat currencies is the coopting of its underlying blockchain technology for other uses, including digital fiat currencies issued by sovereign states. The Bank of England seems to be a leader among central banks in this area, having:

> carried out a distributed ledger technology proof of concept as part of a multi-year research programme into the implications of a central bank, like the Bank of England, issuing a digital currency.
>
> At the moment, the Bank of England provides electronic accounts to banks and key financial institutions, but the public can only hold central bank money in physical form – as banknotes. If a central bank were to issue a digital currency everyone, including businesses, households and financial institutions other than banks, could store value and make payments in electronic central bank money in addition to being able to pay with cash.
>
> While this may seem like a small change, it could have wide-ranging implications for monetary policy and financial stability.[53]

The U.S. Federal Reserve is researching and speaking about innovations in electronic payment systems, distributed ledger technologies and digital currencies but seems to be proceeding even more cautiously than the Bank of England. The Fed has given no indication that it agrees with the various commentators who predict that the Fed will issue its own digital currency in the near future.

Big tech and finance companies, including JP Morgan Chase, Microsoft, Goldman Sachs, Santander and Intel, are investing in a variety of blockchain and digital currency ventures (e.g. Bitcoin's largest competitor, Ethereum and the R3 consortium).[54] Blockchain technology is thriving, but the prospects of cryptocurrencies achieving a

52 Higgins, Stan, "SEC Denies SolidX Bitcoin ETF Proposal," *Coindesk.com* (March 28, 2017). http://www.coindesk.com/sec-denies-solidx-bitcoin-etf-proposal/

53 "Digital Currencies," in *Bank of England*, http://www.bankofengland.co.uk/research/Pages/onebank/cbdc.aspx/ Accessed May 8, 2017.

54 Hackett, Robert, "Big Business Giants From Microsoft to J.P. Morgan Are Getting Behind Ethereum," *Fortune*, (February 27, 2017). http://fortune.com/2017/02/28/ethereum-jpmorgan-microsoft-alliance/

liberation of the global monetary system from government control does not appear imminent.

Conclusion

In this paper we have merely scratched the surface of the ontology of money and bitcoins. Bitcoins, and cryptocurrencies generally, overlap in extensive ways with the many sometimes complementary but often contradictory definitions of money. Bitcoin the system and bitcoin the unit of account are money in that they are artifact and concept, mechanized mathematical process and social practice. Perhaps the most intriguing inherent conflict present in Bitcoin/bitcoin is between its social roots and construction and its partly antisocial ideology. We conclude that Bitcoin/bitcoin is already part of the history of money and of its foreseeable future.

Bibliography

Beigel,Ofir, "Is Bitcoin Mining Profitable in 2017?" 99 Bitcoins (March 8, 2017). https://99bitcoins.com/bitcoin-mining-profitable-beginners-explanation/

Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. "Bitcoin: Economics, Technology, and Governance." The Journal of Economic Perspectives 29, no. 2 (Spring 2015): 213-38.

Chaum, David, 1982. "Blind Signatures for Untraceable Payments," CRYPTO '82: Proceedings of the 2nd Conference on Advances in Cryptology (1982), 199–203.

Chaum, David L., 1981. "Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms," Communications of the ACM, 24, no. 2 (February, 1981) 84-90.

Chavez-Dreyfuss, Gertrude. 2017, "LedgerX Gets U.S. Approval for Derivatives on Digital Currencies." U.S. Reuters (July 24, 2017). https://www.reuters.com/article/us-usa-cftc-digitalcurrency/ledgerx-gets-u-s-approval-for-derivatives-on-digital-currencies-idUSKBN1A92FZ

"Controlled supply," in bitcoinwiki, https://en.bitcoin.it/wiki/Controlled_supply Accessed March 19, 2018.

"Digital Currencies," in Bank of England, http://www.bankofengland.co.uk/research/Pages/onebank/cbdc.aspx Accessed May 8, 2017.

Dai, Wei, "B-Money," (1988). http://www.weidai.com/bmoney.txt

Dai, Wei, "Wei_Dai comments on AALWA: Ask any Less Wronger anything," Less Wrong, A community blog devoted to refining the art of human rationality, (January 12, 2014). http://lesswrong.com/lw/jgz/aalwa_ask_any_lesswronger_anything/ap3c

Ferro, Shane, "The alleged Bitcoin founder went to law school for fun — and that says a lot about what Bitcoin is really for," Business Insider (May 15, 2015). http://www.businessinsider.com/bitcoin-is-about-property-law-2015-5

Hackett, Robert, "Big Business Giants From Microsoft to J.P. Morgan Are Getting Behind Ethereum," Fortune (February 27, 2017). http://fortune.com/2017/02/28/ethereum-jpmorgan-microsoft-alliance/

Higgins, Stan, "SEC Denies SolidX Bitcoin ETF Proposal," Coindesk,com (March 28, 2017). http://www.coindesk.com/sec-denies-solidx-bitcoin-etf-proposal/

Hill, Kashmir, "Federal Judge Rules Bitcoin Is Real Money," Forbes (August 7, 2013). https://www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-bitcoin-is-real-money/#1acf9a8a27b8

Koschate-Fischer, N. & Wüllner, K. Journal of Business Economics (2017) 87: 809. https://doi.org/10.1007/s11573-016-0839-z

Krugman, Paul, "Bitcoin Is Evil," The New York Times (December 28, 2013) https://krugman.blogs.nytimes.com/?s=bitcoin

Manne, Robert, "The Cypherpunk Revolutionary," The Monthly (March 2011). https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary

May, Timothy C., The Crypto Anarchist Manifesto (November 22, 1992). https://www.activism.net/cypherpunk/crypto-anarchy.html,

Meyer, Gregory, "US derivatives regulator looks to calm cryptocurrency fears," The Financial Times (January 31, 2018). https://www.ft.com/content/db9d547e-06b4-11e8-9650-9c0ad2d7c5b5

Mises, Ludwig von, "Part Four: Catallactics or Economics of the Market Society, Chapter XVII. Indirect Exchange," in Human Action (1940), 778. https://mises.org/library/human-action-0/html/pp/778

Mises, Ludwig von, "Part Four: Monetary Reconstruction, Chapter III The Return to Sound Money, § 2 The Integral Gold Standard," in The Theory of Money and Credit (New Haven: Yale University Press, 1953), 438. https://mises.org/system/tdf/The%20Theory%20of%20Money%20and%20Credit_3.pdf?file=1&type=document

Murphy, Hannah, "Regulators eye ban on cryptocurrency derivatives bitcoin," The Financial Times (January 18, 2018). https://www.ft.com/content/d6df33a0-fc4e-11e7-9b32-d7d59aace167

Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, (October 31, 2008). https://bitcoin.org/bitcoin.pdf

Popper, Nathaniel, "Mt. Gox Creditors Seek Trillions Where There Are only Millions," The New York Times (May 25, 2016). https://www.nytimes.com/2016/05/26/business/

dealbook/mt-gox-creditors-seek-trillions-where-there-are-only-millions.html?_r=0

Raskin, Max and David Yermack, "Digital Currencies, Decentralized Ledgers, And The Future Of Central Banking," NBER (National Bureau of Economic Research) Working Paper 22238 (May 2016). http://proxy.library.upenn.edu:3290/papers/w22238.pdf

Ron, Dorit, and Adi Shamir. "Quantitative analysis of the full bitcoin transaction graph." In International Conference on Financial Cryptography and Data Security, pp. 6-24. Springer, Berlin, Heidelberg, 2013.

Simmel, Georg, The Philosophy of Money, 3rd ed., ed. and trans. by David Frisby. London: Routledge, 2004.

Southurst, John, "Hal Finney Passes Away," Coindesk,com (August 29, 2014). http://www.coindesk.com/bitcoin-pioneer-hal-finney-passes-away/

St. Onge, Peter, "Cryptocurrencies and a Wider Regression Theorem," Mises Institute (December 11, 2014). https://mises.org/library/cryptocurrencies-and-wider-regression-theorem

Szabo, Nick, "Bit gold," Unenumerated, An unending variety of topics (December 27, 2008). http://unenumerated.blogspot.com/2005/12/bit-gold.html

Szabo, Nick, "Formalizing and Securing Relationships on Public Networks," first monday, Peer Reviewed Journal On The Internet, 2, no. 9 (September 1, 1997). http://firstmonday.org/ojs/index.php/fm/article/view/548/469#Conclusion

Tschorsch, Florian and Björn Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," IEEE Communications Surveys & Tutorials, 18, no.3, (March 2, 2016), 2084-2123.

Yermack, David, "Is Bitcoin a Real Currency? An Economic Appraisal," NBER (National Bureau of Economic Research) Working Paper 19747 (December 2013). http://www.nber.org/papers/w19747