Cryptocurrencies Change Everything

Alexander Lipton
The Jerusalem School of Business Administration
HUJI, Jerusalem, Israel
Connection Science and Engineering
MIT, Cambridge, MA, USA
SilaMoney, Portland, OR, USA
alexlipt@mit.edu

July 2, 2021

Abstract

New technologies unleashes competitive threats to the incumbents by allowing new entrants to join the party and eventually reshape the entire financial ecosystem

1 Introduction

I vividly remember my experience in January 2020 at the World Economic Forum in Davos, which I attended as part of the MIT Connection Science contingent. Since Davos is a small town, ill-suited for hosting large international gatherings, space was at a premium. Before giving a scheduled interview, I had to wait in a small room for the previous conversation to finish. The interviewee was very hostile to cryptocurrencies and used obligatory references to the infamous tulipmania and profane language to make his points.

The longer the interview lasted, the clearer it became to me that this distinguished scholar had little, if any, understanding of the topic he was talking about. He compensated for the lack of knowledge with his strong language, which, unfortunately, is not uncommon when cryptocurrencies and distributed ledgers are discussed. I mentally called the professor a "*sans-cluelotte*," i.e., a person without a clue.[1]

This experience is still fresh in my memory after more than a year. Hence, when the editors of Quantitative Finance invited me to write a piece explaining my views of cryptocurrencies, blockchains, distributed ledgers, and "all this jazz," I accepted their invitation with alacrity. Here are the fruits of my labor.

[1] Recall that in late 18th-century France, the *sans-culottes* were the commoners actively participating in the French Revolution. I was pleased to see - No results found - as an outcome of my Google search for "*sans-cluelotte*".

Interested readers can find further details in a recent book written by Adrien Treccani and me; see Lipton and Treccani (2021).

2 Existing financial system and its painpoints

The existing financial system is too complex for its own good. This complexity arises for several reasons. First and foremost, historically, banks commit the cardinal sin of capitalism by violating the division of labor and engaging in record keeping and credit creation *at the same time*.

Second, regulators rely on macroeconomic theories, which are manifestly wrong and do not pass muster with thinkers raised on scientific tradition; see Lipton (2016a). As a result, they use obsolete and imprecise tools for steering economic activities in the desired direction. Reliance on negative interest rates and dogged pursuit of Quantitative Easing (QE) are just two of many examples.

Exceptionally low or negative interest rates are destroying the middle class, with little benefit for society at large. They exacerbate the inequality, which has been growing exponentially. QE is forcing central banks to alter their *modus operandi* dramatically and become fractional-reserve banks in all but name. One can reuse the apt phrase of Ferdinand Braudel and describe the financial system as "*un total de faiblesses.*"[2]

The Global Financial Crisis (GFC) was an excellent but wasted opportunity to reorganize the world financial ecosystem. Rather than shrinking, too-big-to-fail banks became even more prominent than before the crisis and massively increased their overall business share. Although undeniably better capitalized, banking institutions are so complex that regulators, depositors, investors, or even internal management do not understand their balance sheets' complexity in detail. As a result, bank conglomerates morphed into institutions, which are too-big-to-manage, and, even more, alarmingly, too-big-to-regulate. Examples abound. In 2020 - 2021, Citibank erroneously paid principal instead of interest and lost half-a-billion dollars as a result; Credit Suisse lost five billion dollars on an Archegos margin call; Robinhood, who received a broker-dealer license without being able to calculate initial margins correctly, was forced to raise billions of dollars overnight to deliver them to its clearinghouse. One can extend this list *ad nauseam*. Cato the Elder put it best: "*Carthago delenda est.*"[3]

3 Satoshi Nakamoto as a magisterial reformer

3.1 Money

Before talking about Bitcoin, we need to talk about money. Money plays a vital role in modern society. It is simultaneously very concrete and abstract. There is no doubt in my mind that money is one of the greatest inventions

[2] A total of weaknesses.
[3] Carthage must be destroyed.

of humankind, on a par with writing. Speaking of which, the Sumerians invented writing first and foremost to reflect economic and monetary relations; see Goetzmann (2017). While reasonable people can disagree about some attributes of money, several of its main properties are beyond dispute. Money has to be: (A) a medium of exchange; (B) a means of payments; (C) a store of value; (D) a unit of account. Given the above, money can be viewed as a perpetual call option for acquiring goods and services and discharging one's obligations. In contrast to paying with cryptocurrencies, paying with money is not a taxable event per se. Besides, Graziani (2003) and Keen (2001) argue that in a monetary (as opposite to a barter) economy, money has to be: (A) represented by a token; (B) accepted as a means of final settlement of all transactions terminating all credit and debt relationships between the parties; (C) seigniorage-neutral, i.e., not granting privileges of seigniorage to any agent making a payment, thus requiring the presence of a bank as a third party to any non-cash transaction. Okamoto and Ohta (1991) succinctly articulate requirements for electronic money as follows. Electronic money is: (A) securely usable online (online payment); (B) securely usable offline (offline payment); (C) transactable without revealing parties' identities (anonymity or pseudonymity); (D) transferrable to others (transferability); (E) subdivisible as needed (divisibility); (F) not copiable or reusable (non-reproducibility).

Historically, anything acceptable for discharging tax obligations eventually became money. Wicksteed (1910) summarizes the situation best: "Inconvertible paper money had a positive value squarely on its being made acceptable by the government for the payment of taxes."Since money and taxes come hand-in-hand, in a modern, legally compliant economy, money has to be linked to identity one way or the other.

Money can be object-based, such as gold coins or banknotes, or record-based, such as bank deposits. Interestingly enough, in ancient Mesopotamia, priests made progress toward using record-based money. While it was widely used in antiquity, record-based money was more or less forgotten for a thousand years. Money was predominantly object-based in the Middle Ages. However, over time, it became clear that object-based money is not commensurable with the growing complexity of the economic system, so that record-based money became prevalent again. Initially, it took hold in Venice and Genoa in Italy and then spread through Lyon to the Low Countries, specifically Belgium and the Netherlands. Then it expanded to London, Paris, Zurich, New York, Tokyo, etc.

As a result, people and their money became separated, and intermediary handling the money became the central part of the system, rather than its auxiliary. Essentially, the financial system was modeled on the Catholic Church's organization. Since ordinary Catholics could not read the Bible themselves because it was written in Latin, a priest had to interpret the Bible for them. Similarly, unless a person pays in cash, they have to rely on a banker to make a payment. Essentially, if Alice and Bob wanted to exchange some value, it wouldn't be directly between Alice and Bob. Instead, the transaction would be between Alice and her banker, then Alice's and Bob's bankers, and Bob's banker

and Bob. This chain is even more complicated when cross-border payments are involved.

3.2 Bitcoin protocol - switching from analog to digital cash

In a message to the Cryptography Mailing List, sent in 2008, Satoshi Nakamoto stated: "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party – The main properties: Double-spending is prevented with a peer-to-peer network. No mint or other trusted parties. Participants can be anonymous. New coins are made from Hashcash style proof-of-work. The proof-of-work for new coin generation also powers the network to prevent double-spending."

In my mind, Nakamoto is a magisterial reformer in the mold of Martin Luther, John Calvin and their collaborators. Recall that the Reformation made a crucial point of translating the Bible from Latin to vernacular, allowing an individual to read it and understand its meaning directly rather than rely on a priest. Similarly, Nakamoto's bold idea allowed to move value via the Internet in a peer-to-peer fashion, theoretically eliminating the need for a banker.

In the ideal world envisioned by Satoshi Nakamoto, Alice can send BTC from her address to Bob's address, thus discharging her obligations. Essentially there are no more bankers in between, provided that Alice and Bob know how to handle their wallets, secret keys, etc. However, managing security, which is paramount for the success of the whole model, is by no means simple at an individual's level and even more complex for an organization.

This type of value transfer is an idealized construct. What we see right now is that direct usage of BTC as money is not still quite possible. In reality, for ordinary people to get BTCs (or other cryptocurrencies), they have to become clients of a centralized exchange, such as Coinbase, Kraken, and myriad others. To make Bitcoin truly decentralized, one needs to create a system allowing earning and spending Bitcoins or other cryptocurrencies in a decentralized fashion.

The Bitcoin protocol, which was launched in January 2009 by S. Nakamoto, is simultaneously complex and simple. Surprisingly, it does not use novel cryptographic primitives, relying instead on the tried-and-tested tools, such as public key infrastructure, Merkle trees, hash functions, proof-of-work, and several auxiliary ones; see Lipton and Treccani (2021).

In a nutshell, the Bitcoin protocol can be summarized as follows; see Nakamoto (2008). The objective is to create an alternative currency, with BTC being its native unit, tradable peer-to-peer.[4] The protocol utilizes the unspent transaction output accounting. The sole purpose of Bitcoin transactions is to move BTC from one address to another. It is implemented on a public blockchain using elliptic curve secp256k1. All Bitcoin addresses are secret-key controlled; the

[4] We would like to emphasize again that, in reality, the vast majority of BTC trading occurs on centralized exchanges.

ownership of an address (and all the associated BTCs) is proven via an elliptic curve digital signature algorithm (ECDSA). Blockchain consensus is maintained via a Proof-of-Work (PoW) algorithm using the SHA256 hash function. Consensus keepers are miners and full nodes. Miners assemble transactions into blocks containing approximately 2,000 transactions (TXs) each and verify them by solving PoW puzzles. For their efforts, miners receive block rewards and voluntary transaction fees. Block mining time is about 10 min. Verified blocks grow on top of each other to form a blockchain. The bitcoin transacted currency (BTC) supply mechanism is solely through mining rewards. Initially, mining rewards were 50 BTCs; currently, they are 6.25 BTCs. Rewards are halved after each set of 210,000 blocks is mined, which caps supply at 21 million BTC in total. Thus, the Bitcoin supply style is deflationary.

Like the Greek goddess Aphrodite, who, according to Hesiod's Theogony, was born fully formed near Paphos on the island of Cyprus, the Bitcoin protocol appeared ready to go from day one and has been operational ever since; see Schlegel and Weinfield (2006); Nakamoto (2008). It is truly remarkable, given the slow and buggy development of other software projects. However, when I first read Nakamoto's seminal paper and later studied the associated protocol, I could not help but notice some similarities between Nakamoto's vision and the infamous Schlieffen plan. Recall that Count Alfred v. Schlieffen devised this plan for a war-winning offensive against France; however, he never thought it through in detail. Schlieffen conveniently ignored the fact that Germany did not have enough troops to execute the plan on the ground and that logistic difficulties were unsurmountable. As a result, when the plan was implemented in 1914, it failed; see van Creveld (1977). Likewise, Nakamoto says nothing about what would happen when the block rewards become de minimus, which might be the weakest part of the vision.

Moreover, one needs to be aware of the fact that Nakamoto created a self-consistent world, which is not directly connected to the real world. Hence, the price of BTC can and does fluctuates very widely. Conceptually, the Bitcoin protocol was the first successful attempt to switch from cash, which is an analog instrument, to BTC, a digital instrument.

3.3 Bitcoin protocol - pros and cons

Bitcoin's idealists envisioned a brave new world, such that:

1. BTC will be an efficient means of peer-to-peer payments on a global scale.
2. Goods and services will be priced in BTC.
3. BTC mining and associated energy consumption will be moderate in scale; anyone could be a BTC miner and BTC consumer.
4. BTC will be usable by all, with the vast majority of transactions executed for legitimate purposes.

5. The community will support BTC at large rather than any particular government or private company.

6. The Bitcoin protocol would only need minor updates decided upon by the community of Bitcoin Core developers.

Bitcoin's detractors and supporters are engaged in never-ending heated debates over its cons and pros.

Pessimists claim; see, e.g., Rubini (2018):

1. Sluggisheness of the underlying protocol makes Bitcoin not suitable as a means of payment.

2. Price volatility in terms of fiat currencies prevents Bitcoin from being a store of value or a unit of account.

3. Bitcoin's reliance on the proof-of-work and mining wastes energy on an immense scale.

4. Perceived anonymity of Bitcoin encourages its usage for nefarious activities.

5. Bitcoin's lack of backing makes it worthless.

6. Sooner or later, the protocol drawbacks will result in a competitor replacing it as a top cryptocurrency.

Optimists respond as follows; see, e.g., Bhutoria (2020):

1. Bitcoin is capacity-constrained by design and deliberately optimizes its limited capacity by emphasizing the settlement of large transactions outside of the conventional financial system.

2. Bitcoin's volatility will decrease with its greater adoption as an asset class and the development of Bitcoin's derivatives.

3. Bitcoin mining primarily relies on renewable energy; Bitcoin's network utilization of electricity is a legitimate use of natural resources.

4. Bitcoin is a protocol, i.e., a neutral tool with properties valuable to good actors and bad actors alike, like the Internet; in any case, the share of the illicit Bitcoin transactions is low.

5. Although Bitcoin has no associated cash flows, industrial utility, or legal standing, it is backed by its scarcity, being an integral part of the Bitcoin protocol. It can be viewed as "digital gold."

6. While one can easily alter Bitcoin's software because it is open-source, it is impossible to recreate the associated community and network effects.

Realists see the truth somewhere in-between; see Lipton and Treccani (2021):

1. The Bitcoin protocol cannot be used for conventional payments because it processes only about 3-6 Transactions-per-Second (TpS), while Visa processes 20,000 TpS. Thus paying for your coffee with BTCs is out of the question. Still, one can use BTC for the immutable and final discharge of substantial obligations.

2. Undeniably, the BTC price is prone to periodic bubble-bust episodes, so that it is hard to use Bitcoin as a conventional store of value. However, the overall number of BTCs is limited, and most of them are held mainly by the so-called HODLERs (sic), unwilling to part with their BTCs. Thus, BTC is likely to retain some residual value for the foreseeable future, allowing investors with long-term horizons to use it for storage.

3. According to University of Cambridge estimates, in 2019 the Bitcoin protocol used an estimated 62 terawatt-hours of electricity - more than such countries as Switzerland and the Czech Republic; about 0.28% of the total global electricity consumption - unquestionably, an enormous amount of energy, given that in 2019 the protocol processed only 120 million transactions. Although such profligacy looks like sheer madness for the uninitiated, the protocol's very nature dictates that energy wastage is the only way for maintaining its integrity. Energy consumption is a crucial feature, which will determine Bitcoin's long-term viability. If Bitcoin can rely on renewable electricity, it can survive in the long term; if not, its days are numbered. It is worth noting that BTC mining in Iceland, frequently mentioned as an example of green BTC mining, is running into unsurmountable capacity constraints.

4. There is no question that criminals often use BTC for nefarious purposes, such as collecting ransoms, evading capital controls, etc. However, whenever possible, they use cash and the banking system on a much larger scale. Several events, such as the Danske Bank money laundering scandal, resulting in €200 billion laundered between 2007 to 2015, help put matters in perspective.

5. BTC has no intrinsic value. Thus, it is better to think of it as a club membership. There are a fixed number of memberships and many potentially interested parties, which is enough to maintain the memberships' value in the long run. In addition to financial gains or losses from trading in their membership rights, the players also receive entertainment value and boasting rights from owning their BTCs.[5] By contrast, according to Aristotle, conventional money is derived from the law and, hence, coercion rather than fun.[6] The fact that BTC can be a store of value is not

[5] Additional value of Bitcoin stems from the fact that one can use it as a convincing counterexample in macroeconomics. Even a cursory look at the BTC price chart shows that the celebrated efficient market hypothesis makes no sense at all.

[6] Aristotle articulated legal aspects of money, emphasizing that money and government are joined at the hip, Crisp (2014): "[M]oney has been introduced by convention as a kind of substitute for need or demand, and this is why we call it money ($\nu o \mu \iota \sigma \mu \alpha$) because its value

particularly surprising *per se*. Numerous assets can be stores of value for reasons other than their direct usefulness. Gold is an excellent example of such an asset: it has been an attractive store of value since time immemorial despite its limited utility for most industrial applications. Art is the same, especially modern art. Fiat money, which replaced gold after a period of coexistence lasting for hundreds of years, is a store of value despite being a depreciating asset. The fact that BTC has no intrinsic value implies that it can have any price.

6. One cannot be sure that Bitcoin will be around a hundred years from now. Yet, since its inception, Bitcoin has proven its astonishing resilience, being unique in many ways, such as scarcity, adoption rate, robustness, and trust. It is improbable that Bitcoin will be superseded by a more robust and less wasteful technology in the near to medium time horizon. However, it is more likely to be replaced by a more compelling and less wasteful technology in the more distant future. One can draw an analogy between Bitcoin and vinyl discs. Although there are many ardent fans of vinyl discs, their community has shrunk dramatically since their prime days. The real danger for Bitcoin's very existence is possible government intervention, triggered either by its freewheeling ways or, more likely, excessive energy consumption. When proponents argue that the distributed nature of the Bitcoin protocol makes it impervious to external interventions, they conveniently omit the fact that miners' operations are squarely based in the real world and can be disrupted or shut down at will.

4 Beyond Bitcoin

4.1 Background

By developing the Bitcoin protocol, Satoshi Nakamoto opened the floodgates of unprecedented creativity. Bitcoin launched the blockchain revolution by inspiring dozens of protocols and thousands of cryptocurrencies, some feeble or even mischievous imitations, some genuinely new. In this section, we briefly discuss some of these innovations.

4.2 The Ethereum protocol

Ethereum is a genuine attempt to address the limitations of Bitcoin scripts and distributed ledger technology (DLT) in general. The introduction of complete state and Turing-complete scripts called smart contracts allows Ethereum to expand previous-generation distributed ledger technology capabilities and possible applications. Whereas Bitcoin focuses on a single use case of transferring BTCs from one address to another, Ethereum offers a decentralized, trusted computing platform capable of executing an arbitrary code. ETH, Ethereum's

is derived, not from nature, but from the law ($\nu o \mu o \varsigma$), and can be altered or abolished at will."

native cryptocurrency, is not an end in itself: it merely acts as the token financing the execution of smart contracts that regulate the flows of entirely separate use cases by thousands of machines. An Ethereum white paper boldly claims: "What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code."

The Ethereum protocol was launched by V. Buterin, G. Wood, J. Lubin, et al. in July 2015. The protocol uses the same cryptographic primitives as Bitcoin. In brief, it can be summarized as follows; see Buterin (2013); Wood (2015); Lipton and Treccani (2021). The objective of the Ethereum protocol is to create a distributed world computer, with ETH being its native token, tradable peer-to-peer, and usable for paying for the execution of smart contracts.[7] The protocol utilizes account-based accounting. The purpose of Ethereum transactions is either moving ETH from one address to another or executing a smart contract. It is implemented on a public blockchain using elliptic curve secp256k1. Ethereum addresses are either secret-key controlled or correspond to smart contracts; the ownership of an address (and all the associated ETHs) is proven via an ECDSA. Blockchain consensus is maintained via a PoW algorithm using the Ethash hash function (Ethereum aims to switch from the PoW to the Proof-of-Stake algorithm). Consensus keepers are miners and full nodes. Miners assemble transactions into blocks containing approximately 380 TXs each and verify them by solving PoW puzzles. For their efforts, miners receive block rewards and mandatory transaction fees paid in gas. Block mining time is about 15 sec. Verified blocks grow on top of each other to form a blockchain. The ETH supply mechanism relies on a combination of pre-mined supply and mining. Currently, mining rewards are 2 ETHs per block. Supply is capped at 18 million ETH per year. Thus, the Ethereum supply style is inflationary.

Ethereum can be viewed as a consensus as a service (CaaS) provider. As such, it can be used to build new smart-contract-based tokens very quickly.[8] Moreover, the protocol does have an Achilles heel - it is self-contradictory and self-defeating because the higher the ETH price goes, the less suitable Ethereum becomes as a CaaS provider. As a result, the Ethereum protocol is too expensive to use! The pay-per-operation model, utilized by the protocol, is archaic and reminds one of the infamous pay-per-minute billing utilized by telephone companies in the 20th century. Thus, other, less expensive approaches are needed to build genuinely versatile CaaS protocols.

4.3 Other protocols

Numerous protocols have been developed over the last decade to address actual or perceived deficiencies of Bitcoin and Ethereum as well as for the fun of it.

[7] In actuality, ETH is primarily traded on exchanges.

[8] Despite their name, smart contracts are not particularly smart and require massive quantities of collateral for their operation.

A promising direction is to build either practical Byzantine fault-tolerant or directed acyclic graph protocols because they are much cheaper to execute than their PoW-based brethren.

4.4 CBDCs

As was mentioned earlier, one can view the BTC as a digital version of cash. Of course, as discussed earlier, it is not perfect by any stretch of the imagination. Still, the very existence and robustness of the Bitcoin protocol show that one can digitize cash.

One promising avenue is building the so-called central bank digital cash (CBDC). As its name suggests, CBDC has to be created by central banks. Central banks can try to do it directly or delegate it to private banks, which would operate under central banks' supervision. At present, the People's Bank of China is actively developing China's Digital Currency Electronic Payment infrastructure. Several smaller nations are about to release theirs, and many others, including the Federal Reserve, are exploring various approaches to developing their CDBCs. Several years ago, Lipton (2016b) pointed out the delegation of responsibilities by central banks to private banks issuing CBDCs is the most likely outcome. The crucial features of any successful CBDC protocol are high throughput, extreme robustness, and, not surprisingly, the ability to process transactions offline. It is possible that, instead of relying on distributed ledgers, CBDCs can be based on the blind signature paradigm of David Chaum; see Chaum (1983).

4.5 Stable coins

Rather than waiting for central banks to digitize cash on their own, many entrepreneurs decided to act independently by developing the so-called stable coins, i.e., cryptocurrencies with prices oscillating in very narrow bands around the corresponding fiat currencies. The top stable coins by capitalization are Tether, USD Coin, Binance USD, and DAI. The first three are claimed to be fully collateralized with fiat currency; the fourth one is overcollateralized with ETH. These coins are better suited for trading on crypto exchanges. Some smaller stable coins, such as Sila, are designed to be used for the needs of the real economy.[9]

4.6 DeFi

Using CaaS providers, such as Ethereum, one can digitize financial instruments other than cash and build decentralized finance (DeFi), which utilizes the corresponding smart contracts and is independent of the intermediaries, such as banks, exchanges, and brokers. For example, one can design a smart-contract-based exchange, defined by simple mechanical rules, which can work as well or

[9] In the interest of full disclosure, I am a co-founder and CIO of Sila.

better than traditional market-makers. One can envision full-scale decentralized exchanges (DEX), replacing central clearing counterparties and providing real-time, rather than $T+2$, clearance and settlement. One can argue that such an infrastructure would help to reduce the fallout from the Archegos debacle and similar episodes. More boldly, one can replace the existing infrastructure with automated market makers. For further details, see Feenan *et al.* (2021) and references therein.

5 Conclusion

It is impossible to reform the existing system using old technologies. Thankfully, the introduction of new technologies, described above, unleashes competitive threats to the incumbents allowing new entrants to join the party and eventually reshape the entire financial ecosystem. The reinvention of financial services will be pivotal for building a new economy by helping to increase efficiency, reduce inequality, and fund the required infrastructure. More broadly, DLT will create new approaches for better digital privacy and cybersecurity, more inclusive and resilient civic and government systems, and more flexible and transparent responses to society's problems; see Pentland et al. (2021).

At present, several major competitive races take place: (A) cash *vs.* cryptocurrencies; (B) centralized *vs.* distributed payment systems; (C) centralized *vs.* distributed market infrastructures; (D) fractional-reserve *vs.* narrow banks. I put my money on newcomers. How about you?

Acknowledgment *I am grateful to Dr. Alexander Eydeland, Prof. David Gershon, Dr. Thomas Hardjono, Mr. Shamir Karkal, Dr. Marsha Lipton, Prof. Alex (Sandy) Pentland, and Dr. Adrien Treccani for many valuable conversations. I wish to thank Prof. Michael Dempster and Prof. Jim Gatheral, joint Editors-in-Chief of Quantitative Finance, for their invitation to write this essay.*

References

Bhutoria, R. (2020). Addressing Persistent Bitcoin Criticisms. In: Fidelity Digital Assets Working Paper.

Buterin, V. (2013). A Next-Generation Smart Contract and Decentralized Application Platform. White Paper. Available online at: https://github.com/ethereum/wiki/wiki.

Chaum, D. (1983). Blind signatures for untraceable payments. *In Advances in Cryptology* (pp. 199-203). Boston, MA: Springer.

Crisp, R. (2014). *Aristotle: Nicomachean ethics.* Cambridge: Cambridge University Press.

Feenan, S., Heller, D., Lipton, A. *et al.* (2021). Decentralized financial market infrastructures: Evolution from intermediated structures to decentralized

structures for financial agreements. *The Journal of FinTech* 1(2), 2150002 (42 pages)

Goetzmann, W.N. (2017). *Money changes everything: how finance made civilization possible.* Princeton: Princeton University Press.

Graziani, A. (2003). *The monetary theory of production.* Cambridge: Cambridge University Press.

Keen, S. (2001). *Debanking economics. the naked emperor of the social sciences.* London and New York: Zed Books.

Lipton, A. (2016a). Macroeconomic Theories: Not Even Wrong. *Risk*, 30(9), p. 29.

Lipton, A. (2016b). The Decline Of The Cash Empire. *Risk*, 30(11), p. 53.

Lipton, A. and Treccani, A. (2021). *Blockchain and Distributed Ledgers.* Singapore: WSPC.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. White Paper. Available online at: https://bitcoin.org/bitcoin.pdf

Okamoto, T. and Ohta, K. (1991). Universal Electronic Cash. In: *Annual International Cryptology Conference, Berlin and Heidelberg*, Springer, pp. 324–337.

Pentland, A, Lipton, A. and Hardjono, T. (2021). Building the New Economy. Cambridge, MA: The MIT Press.

Rubini, N. (2018). Crypto is the mother of all scams and (now busted) bubbles, while blockchain Is the most over-hyped technology ever, no better than a spreadsheet/database. Testimony for the Hearing of the US Senate Committee on Banking, Housing and Community Affairs.

Schlegel, C. and Weinfield, H. (eds.). (2006). Theogony: And, Works and Days. University of Michigan Press, Ann Arbor Michigan, USA

van Creveld, M. (1977) *Supplying War: Logistics from Wallenstein to Patton.* Cambridge University Press, Cambridge, UK.

Wicksteed, P.H. (1910). *The common sense of political economy, including a study of the human basis of economic law.* London: Macmillan.

Wood, G. (2015). Ethereum: A Secure Decentralised Generalised Transaction Ledger Homestead Revision. In: Yellow Paper.