Information Systems Frontiers (2020) 22:17–22
https://doi.org/10.1007/s10796-019-09966-2

# Analyzing Cryptocurrencies

Xiaofan Li[1] · Andrew B. Whinston[1]

Published online: 28 November 2019
© Springer Science+Business Media, LLC, part of Springer Nature 2019

**Abstract**
Cryptocurrencies, such as Bitcoin, have been an important factor in some economic activities. For example, Bitcoin is the main payment method for ransomware attackers and retailers on the Darknet. It is therefore useful to understand the features of cryptocurrencies and their economic implications. In this research, we use bitcoin, Ether, and XRP, the three cryptocurrencies with the highest market values as of this writing, as well as Libra, which is forthcoming and topical, as examples to analyze their features. Specifically, we argue that these cryptocurrencies are fundamentally different due to differences in the following factors: the identity management of their ledger writers, their consensus algorithms, and their coin supply. We discuss how these factors determine cryptocurrency performance, including security, privacy, and financial influence. We also discuss potential research topics around these cryptocurrencies that are still open.

**Keywords** Blockchain · Cryptocurrency · Bitcoin · XRP · Ether · Libra

## 1 Introduction

Digital currencies are a category of currencies that are available in digital form. In contrast to traditional currencies, such as fiat currencies, transactions with digital currency are usually much faster, as well as borderless. Tencent's QQ coin, introduced in early 2005, is one of the pioneers of digital currency. Cryptocurrencies are digital currencies whose ownership can be proved exclusively cryptographically. Cryptocurrencies have been an important factor in some economic activities. For example, Bitcoin is the main payment method for ransomware attackers and retailers on the Darknet. Apple also introduced its cryptocurrency wallet, CryptoKit, since cryptocurrencies are expected to be more widely used in the future.

The ownership and transactions of cryptocurrencies are recorded on distributed ledgers, typically blockchains. The security and integrity of traditional ledgers that record transactions, such as banks' ledgers, are managed by centralized entities, such as banks. In contrast, the security and integrity of the blockchains are usually managed by multiple decentralized writers. When the writers of a ledger disagree on issues regarding the ledger, such as whether a transaction is valid and should therefore be recorded, a consensus algorithm determines how the disagreement is resolved.

Nakamoto (2008) introduced the fundamental blockchain technology, where blocks on the ledger record certain transactions. Each block also records the hash of its previous block, which is determined by the transactions recorded in that previous block. Given this chain structure, if one wanted to edit the transactions in a certain block, all the blocks following that block also need to be edited, creating difficulty in manipulating the blockchain ledger.

With this technology, the first cryptocurrency, Bitcoin, was introduced in 2009. As of this writing, there are more than 1600 cryptocurrencies and the number is growing. Many aspects differentiate these cryptocurrencies, determining each one's performance, including security, privacy, and financial influence. We argue that the fundamental aspects of all cryptocurrencies are the identity management of its ledger writers, its consensus algorithm, and its supply.

The major difference between blockchains and traditional ledgers is the decentralization of writers. Traditional ledgers that record transactions are managed by centralized financial organizations, such as banks, which are responsible for the integrity and security of the ledgers. In contrast, blockchains are managed by decentralized writers. The identity management of these writers is therefore a critical feature of a

✉ Xiaofan Li
li.x@utexas.edu

Andrew B. Whinston
abwhins@gmail.com

[1] McCombs School of Business, University of Texas at Austin, Austin, TX, USA

blockchain. Public blockchains have no identity management; anyone can be a writer. At the other extreme are private blockchains, where a single entity serves as the writer of the blockchain. Between these two categories are permissioned blockchains, where there can be multiple writers, but their identities are managed to some extent by a single entity, who is usually the initiator of the permissioned blockchain.

Another critical feature of a blockchain is its consensus algorithm. A consensus algorithm is a mechanism through which writers reach a consensus about the validity of transactions. This is especially important for public blockchains because, in the absence of identity management, the consensus algorithm is the only mechanism incentivizing the writers to record valid transactions.

A cryptocurrency is usually supplied from two sources. First, some coins are generated over time and awarded to the writers. This source is generally available on public blockchains because the writers of public blockchains need such incentives to work on writing. Second, some coins are endowed to the initiator of the cryptocurrency at the time of initiation. Usually, there is an initial coin offering (ICO) for such cryptocurrencies such that they are publicly traded. A cryptocurrency's supply could be either one or both of these sources.

In this research, as examples, we analyze bitcoin, Ether, and XRP, the three cryptocurrencies with the highest market value as of this writing, as well as Libra, which is forthcoming and topical, from the aspects mentioned above to discuss the issues around these fundamental settings of a cryptocurrency. We also explore potentially interesting research topics around both the analyzed cryptocurrencies themselves and their settings.

## 2 Bitcoin

### 2.1 Proof-of-Work System

Bitcoin, as the first cryptocurrency, is based on a public blockchain, the Bitcoin network. The consensus algorithm that the Bitcoin network uses is a proof-of-work system, which is also the most common consensus algorithm for public blockchains.

A hash function is a mathematical algorithm that maps data into a string of a fixed size, which is called the hash value, or hash. Generally, for blockchains, a block's data include the transactions recorded and the hash of the previous block. Therefore, to write a new block, the hash of the previous block needs to be found.

In proof-of-work systems, a block's hash is designed to be computationally challenging to determine, such that a writer needs to show his or her own proof of work, which is the determination of the hash, to edit that block and subsequent blocks. Specifically, in the Bitcoin network, computational difficulty is created by adding a meaningless numerical value, also known as a nonce, to a block's data and restricting the block's hash to below target number. To determine a valid hash that is small enough, the nonce must be randomly guessed and the hash value for each nonce calculated in combination with the other data in the block. The computational power to determine the hash is therefore used to compute the hash functions and is measured by the hash rate, which is the number of hash functions calculated per unit time.

Generally, in all blockchains, not all the transactions recorded in the blocks are considered valid. Only one chain of blocks, called the ledger of consensus, is considered valid. In other words, when multiple different blocks follow the same block, at most one of them is considered valid. This phenomenon is known as forking, and the different blocks, combined with the blocks following each of them, are called forks. In the Bitcoin network, the longest fork, that is, the one with the most blocks, is considered the ledger of consensus. Therefore, when there are multiple competing forks, the one with the greatest hash rate will be the longest asymptotically and thus be the ledger of consensus. In other words, when there is disagreement among the writers, the proof-of-work system is analogous to a voting system in which the number of votes each writer has is proportional to the computational power the writer controls, and the fork with the most votes is the winning fork.

### 2.2 Security: The Double Spending Problem

Double spending, where the same money is spent twice, has always been a concern in writing ledgers, including traditional ledgers. However, for public blockchains, double spending attacks, where an attacker intentionally double spends, are a particularly important issue, because the only defense against them is the consensus algorithm. Traditional defenses, including identity management and centralized control, are not available to public blockchains.

Nakamoto (2008) shows that, in proof-of-work systems, an attacker controlling less than half of the hash rate has a very low probability of a successful double spending attack, whereas an attacker controlling more than half of the hash rate has a very high probability of a successful attack. Nakamoto claims that it is very costly for an entity to own more than half of the hash rate and, even if this is the case, it is not in the entity's interest to conduct a double spending attack because such an attack will undermine the entity's investment in the coins and mining hardware.

However, decentralization does not necessarily mean independence, especially when the number of significant writers of a blockchain platform is relatively small.[1] The writers could

[1] See https://www.blockchain.com/en/stats.

form coalitions to conduct a double spending attack. Li and Whinston (2019a) discuss this possibility for public blockchains with proof-of-work systems and show that the most cost-effective coalition is a grand coalition, which consists of all the strategic writers. Therefore, there will be an incentive to attack only when the payoff from a successful attack can cover the aggregated preferences of all the writers for the cryptocurrency's security and integrity, which arise from their investments and their businesses' dependence on the cryptocurrency.

The result above suggests that such a blockchain platform is a two-sided market, with one side comprising the cryptocurrency's users and the other side comprising the writers. The cryptocurrency is more secure against double spending attacks when more computational power is working on the ledger or more businesses are dependent on it, thus leading to more demand for the cryptocurrency from its users. Simultaneously, the increase in demand will raise the price and liquidity of the cryptocurrency, thus attracting more investments in computational power and businesses.

Understanding of the security of a public blockchain can be obtained through studying the preferences of its writers. Therefore, it will be interesting to understand how the financial market of cryptocurrency would respond to a security failure, which is relevant to the writers' investments in both the cryptocurrency itself and the computational power. In addition, the role of cryptocurrencies in businesses such as ransomware attacking, which has been dependent on payment in bitcoins, is also relevant, because the business runners will have strong preferences for the security of the blockchain and could become a significant writer to ensure it.

### 2.3 Privacy

Cryptocurrencies can generally provide their users more privacy than traditional currencies due to their different approaches of recording ownership and validating transactions. Cryptocurrencies operate with their users' digital keys. These keys are generated in pairs, consisting of a public key and a private key, and are created and stored by cryptocurrency wallets. Each public key is publicly available and used to generate an address, where the ownership of the cryptocurrency is registered, whereas the private key is never revealed. To authorize a transaction, a digital signature is generated with the private key to show the ownership of the cryptocurrency associated with the public key. The writers are able to check the validity of this signature with the public key, while recovery of the private key from the public key is currently mathematical infeasible. On the other hand, traditional currencies are associated with their owners' personal information, instead of such cryptographic keys. Unless cash is used, traditional currencies' ownership is registered with the owners' personal information in financial institutions such as banks. The transactions through the financial institutions are also authorized with this personal information.

Although cryptocurrencies could provide such privacy, not all of them do, but at least Bitcoin does. Such privacy has both positive and negative effects. On one hand, the transaction data generated by the bitcoin users are not under the control of others, which eliminates the risk of data leakage and allows undertargeting in advertisements to be avoided, the latter of which is not favored by everyone. On the other hand, criminals using Bitcoin are much harder to track. They can even build a reputation associated with their Bitcoin public key (Li and Whinston 2019b). This is why ransomware attackers and retailers of illegal products on the Darknet generally require Bitcoin as the payment method (August et al. 2019; Benjamin et al. 2019).

Privacy generates demand for Bitcoin from both sides mentioned above. If people become more concerned about data leakage and ad targeting, the first side could grow. It will be interesting to understand how marketing can be conducted in cryptocurrency markets with such privacy. What data can be collected and how sellers can build their reputation are open questions.

### 2.4 Supply and Financial Influence

Bitcoin's only supply consists of awards to its writers, which is set at a certain amount per block, 50 bitcoins in the beginning and halved approximately every four years. Therefore, the supply of Bitcoin is stable and not subject to monetary policies, as sovereign currencies are. Currently, the demand for bitcoins comes mainly from the markets with privacy mentioned above and the speculation for it. Such demand fluctuates much more than the demand for major sovereign currencies does. Combined with their stable supply, the value of bitcoins fluctuates significantly, which is not a desired characteristic for a general currency. Bitcoins are therefore not as accepted as sovereign currencies in general markets, and thus have less financial influence.

## 3 XRP

### 3.1 Permissioned Blockchains

In contrast to public blockchains, in permissioned blockchains writers can be under identity management, such as reputation systems. As of this writing, Ripple's XRP has the highest market value among cryptocurrencies with permissioned blockchains.

Compared to the consensus algorithms of public blockchains, those of permissioned blockchains are more heterogeneous. Specifically, XRP involves two kinds of nodes: validating nodes, which participate in the consensus

algorithm, and stock nodes, which are used to store ledger history and protect validating nodes from denial-of-service attacks. Stock nodes do not participate in the consensus algorithm and are under no identity management. The validating nodes are identified and their reputation matters. The more trust a validating node has from other validating nodes, the more power it has in the consensus process. Ripple suggests highly reputable nodes, so that a validating node will trust them by default. Such highly reputable nodes are usually managed by highly reputable organizations, such as universities.

Double spending attacks with XRP are extremely unlikely to be successful, as long as some highly reputable nodes are not compromised, and these nodes are also unlikely to be compromised, because of their reputation in the physical world. In addition, permissioned blockchains have more flexibility in designing the consensus algorithms, and thus usually have a higher tolerance for Byzantine faults (Lamport et al. 1982). Therefore, cryptocurrencies with permissioned blockchains, including XRP, usually have reliable security.

### 3.2 ICOs

Unlike cryptocurrencies based on public blockchains, XRP does not need to award its writers with the cryptocurrency itself to provide incentives. Therefore, the amount of XRP is fixed as its blockchain is created and no more is generated. These XRP coins are owned by the company Ripple, which initiated the XRP blockchain. A proportion of these coins are offered by Ripple for public trading. Many other cryptocurrencies hold such ICOs as well.

In terms of the value of money in monetary theory, Bell (2001) points out two major theories. The first theory was developed by the metallists, who believe that the value of a coin comes from its intrinsic value. Such a coin becomes money because of its features, such as its low storage cost (Kiyotaki and Wright 1989). The other theory was developed by the chartalists, who argue that money does not need to have intrinsic value. For example, Minsky (1986) notes that "everyone can create money; the problem is to get it accepted." Such acceptance of money comes from some service that requires to payment with this money. For example, chartalists argue that sovereign currencies are accepted because governments require taxes to be paid with them. Cryptocurrencies with ICOs are better characterized by chartalist theory than by metallist theory. As an example, XRP is created without much cost, and its value comes from the requirement to using XRP for Ripple's service, which consists of fast and secure cross-border money transactions.

It will be interesting to understand the value of such cryptocurrencies with ICOs from a resale market perspective. XRP can be interpreted as tokens to be served by Ripple, and these tokens are sold in the ICO. The market for XRP can therefore be interpreted as a resale market for tokens that attracts both users and speculators of the service provided by Ripple. Wu et al. (2012) show that such a resale market can be beneficial to the seller of the tokens. Currently, ICOs are often used by companies, including both startups and well-established companies such as Telegram (Popper 2019), to obtain funding. The effect of such a resale market on sellers with a demand for funding is an open question.

## 4 Ether

### 4.1 A Platform for Applications and ICOs

The Ethereum blockchain generalizes the ledger idea so that it records not only the transactions of its native cryptocurrency, Ether, but also those of other digital assets, such as other cryptocurrencies and the in-game assets of video games. In addition, Ethereum provides an environment for programming, such that developers can build applications on it.

Due to the feature of being able to support applications and the transactions of other cryptocurrencies, Ethereum serves as a platform for ICOs. Application developers can initiate their own cryptocurrencies and conduct ICOs through Ethereum to raise funds. Ether is used to buy the cryptocurrencies issued on the Ethereum platform. Therefore, as noted for XRP, Ether's value partly comes from Ethereum's service of being the platform for ICOs.

### 4.2 Smart Contracts

On the transactions of digital assets, Ethereum supports smart contracts, which are contingent contracts that are stored on the blockchain and executed once the conditions are met. The checking of the conditions and the execution of the contracts are validated by the consensus of the writers of the Ethereum blockchain, which are open to the public.

Smart contracts could help solving the issue of mistrust between parties. Traditionally, such parties may go to a trusted escrow. And with smart contracts, the writers play the role of the escrow. Therefore, similar to the security concerns for public blockchains we raised when discussing Bitcoin, smart contracts could also suffer from the concern of the writers being corrupted. Whether the incentives of the writers can be manipulated when executing smart contracts is still an open question.

### 4.3 Proof-of-Stake System

As a public blockchain, Ethereum needs to generate Ether continuously to incentivize its writers. In addition, Ether has its own ICO, which suggests that the two sources of supply of a cryptocurrency can coexist. Currently, the consensus algorithm Ethereum uses is a proof-of-work system that is similar

to Bitcoin's. However, Ethereum is planning to switch to a proof-of-stake system, Ethereum 2.0.

In contrast to proof-of-work systems, where a writer's number of votes is proportional to the writer's computational power, in proof-of-stake systems this number is proportional to the number of coins the writer owns. Therefore, a direct advantage of proof-of-stake systems is that there is no competition from computational power, which is more environmentally friendly. In addition, in proof-of-stake systems, the writers' voting power is correlated more strongly with their investments in the coins. Following the arguments of Li and Whinston (2019a), intuitively, the risk of double spending attacks will be lower. Whether this intuition holds remains to be carefully studied.

## 5 Libra

### 5.1 Stablecoins

Libra, a forthcoming cryptocurrency proposed by Facebook, is a stablecoin, in the sense that each Libra coin is fully backed by the Libra Reserve, which is a collection of low-volatility assets, such as bank deposits and short-term government securities in currencies from stable and reputable central banks. In other words, compared to the cryptocurrencies mentioned above, whose supply is fixed, the supply of Libra is not, because its price is fixed. Therefore, stablecoins cannot be based on public blockchains.

Because stablecoins should be pegged to sovereign currencies by their issuers, their integrity depends on whether the issuers are capable of doing so. For example, Tether, the stablecoin with the largest market value currently, is claimed to be backed by US dollars with a ratio of one to one. However, Tether's value has been volatile due to suspicions about whether it is fully backed. In other words, the integrity of stablecoins depends on the reputation of their issuers.

### 5.2 Financial Influence

Other digital currencies, besides stablecoins, have been backed by sovereign currencies. For example, WeChat Pay and Alipay are fully backed by Chinese currency. Central banks around the world, including those of Sweden and Uruguay, are considering issuing central bank digital currency that is fully backed by their own sovereign currency. Brunnermeier and Niepelt (2019) argue that, if a digital currency is fully backed by and has the same liquidity as a sovereign currency, it will be a perfect substitute for it and will not increase financial risk. These conditions are generally satisfied by WeChat Pay, Alipay, and central bank digital currencies, but not necessarily Libra.

First, as mentioned above, Libra is backed by a collection of low-volatility assets instead of a single currency. Second, by Facebook's intention, Libra's liquidity is not the same as that of any sovereign currency. For example, Libra's white paper says that Libra is designed to help with global needs, aiming to expand how money works for more people around the world. These features prevent Libra from being a perfect substitute for any sovereign currency, and could thus influence the demand for sovereign currencies. Specifically, since Facebook is possibly more reputable than the governments in some developing countries, Libra could be a widely accepted currency there, which would reduce the demand for those sovereign currencies and other currencies that are widely used in these countries, such as US dollar. In addition, the demand for the sovereign currencies included in the Libra Reserve could increase due to demand for Libra. Therefore, widespread use of Libra will influence financial systems, and the repercussions have yet to be explored.

### 5.3 Privacy and Marketing

As a cryptocurrency, Libra could provide privacy, as discussed in the Bitcoin section. However, Facebook is likely to provide the option of associating Libra wallets with Facebook accounts, which contain users' personal information. It will be interesting to study how marketing can be conducted with Libra data and how Facebook will incentivize its users to provide these data by associating their wallets with their Facebook accounts. On the other hand, Libra will also provide an opportunity to study how users will handle the tradeoff between privacy and other incentives, such as convenience.

## 6 Conclusions and Discussions

In this research, we discussed the fundamental features of various cryptocurrencies, including their identity management of ledger writers, consensus algorithms, and coin supply. We used examples of bitcoin, XRP, Ether and Libra to show how the differences in these features determine their performance on security, privacy, and financial influence. Although they are all based on the blockchain technology, these differences in features and performances make their usage in the economy fundamentally different. Therefore, when analyzing a cryptocurrency, it is critical to specify its fundamental features as we discussed to determine what the relevant problems for this cryptocurrency are.

There are still many open questions around cryptocurrencies. Generally, as discussed before, most cryptocurrencies provide their users privacy. However, how transactions are carried out with such privacy could be different to the ones in the traditional settings, because transactionees do not know each other's personal information

and therefore may not trust each other. This setting is also different from online retailing, like on Amazon.com, where although the buyers and sellers do not know each other, but the platform knows both sides and acts as the third party to be trusted. Therefore, it will be interesting to study how transactions are made and how marketing can be done with such privacy.

For cryptocurrencies based on public blockchains, it will be interesting to understand how different consensus algorithms, including proof-of-work system and proof-of-stake system, determine the security of the cryptocurrency against double spending. Specifically, to answer this question, the writers' incentives need to be examined. With these incentives, the analysis of the interactions among the writers could draw upon the political science literature (e.g., Groseclose and Snyder 1996; Banks 2000). The writers' incentives could come from their investments or their businesses that are dependent on the cryptocurrencies, such as being cybercriminals. Therefore, understanding such incentives requires understanding both the financial markets and the businesses empirically and theoretically. However, the privacy that cryptocurrencies provide could be a problem for empirical research on them. It will be interesting to explore what empirical evidence can be found in such a setting.

For cryptocurrencies based on permissioned blockchains, their security are generally ensured by the reputation of their writers. Therefore, we believe that the most interesting topic about these cryptocurrencies are not their security but their value, because they are usually issued through ICOs. These cryptocurrencies have similar features to the issuers' stocks, for example, they raise funds for the issuers and their values are correlated with the issuers' performance. However, these cryptocurrencies also have different features. Each cryptocurrency is usually a token for one kind of service from the issuer and therefore an issuer could issue multiple cryptocurrencies for different service. How the value of these cryptocurrencies are determined remains to be seen. Literature on resale marketing (e.g., Garratt and Tröger (2006)) and crowdsourcing (e.g., Zhao and Zhu (2014)) could provide insights into this area.

Finally, for stablecoins with reputable backing, such as Libra, they could have significant financial influence as a general currency, which is not achieved by any existing cryptocurrency. First, it will be interesting to understand whether they have the features to be general currencies. If so, then from a monetary perspective, how such cryptocurrencies will influence the demand for sovereign currencies and therefore the world economy is an important but open problem. Whether and how analysis of sovereign currencies, e.g., Mundell (1961), could extend to these cryptocurrencies is critical and not clear yet.

## References


August, T., Dao, D., & Niculescu, M. F. (2019). Economics of ransomware attacks. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3351416. Accessed 22 November 2019.

Banks, J. S. (2000). Buying supermajorities in finite legislatures. *American Political Science Review, 94*(3), 677–681.

Bell, S. (2001). The role of the state and the hierarchy of money. *Cambridge Journal of Economics, 25*(2), 149–163.

Benjamin, V., Valacich, J. S., & Chen, H. (2019). DICE-E: A framework for conducting Darknet identification, collection, evaluation with ethics. *MIS Quarterly, 43*(1), 1–22.

Brunnermeier, M. K., & Niepelt, D. (2019). On the equivalence of private and public money. National Bureau of Economic Research no. w25877.

Garratt, R., & Tröger, T. (2006). Speculation in standard auctions with resale. *Econometrica, 74*(3), 753–769.

Groseclose, T., & Snyder, J. M. (1996). Buying supermajorities. *American Political Science Review, 90*(2), 303–315.

Kiyotaki, N., & Wright, R. (1989). On money as a medium of exchange. *Journal of Political Economy, 97*(4), 927–954.

Lamport, L., Shostak, R., & Pease, M. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS), 4*(3), 382–401.

Li, X., & Whinston, A. B. (2019a). Public blockchain security and bribery among its writers. Working paper.

Li, X., & Whinston, A. B. (2019b). Externalities of paying ransom to attackers. Working paper.

Minsky, H. P. (1986). *Stabilizing an unstable economy*. New Haven: Yale University Press.

Mundell, R. A. (1961). A theory of optimum currency areas. *The American Economic Review, 51*(4), 657–665.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available at https://bitcoin.org/bitcoin.pdf.

Popper, N. (2019). Telegram pushes ahead with plans for "gram" cryptocurrency. New York Times, August 27, https://www.nytimes.com/2019/08/27/technology/telegram-cryptocurrency-gram.html. Accessed 22 November 2019.

Wu, R., Geng, X., & Whinston, A. B. (2012). A generalized model of partial resale. *Decision Support Systems, 53*(1), 108–117.

Zhao, Y., & Zhu, Q. (2014). Evaluation on crowdsourcing research: Current status and future direction. *Information Systems Frontiers, 16*(3), 417–434.


**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Xiaofan Li** is a Ph.D. candidate in information systems at University of Texas at Austin. His research interest includes cybersecurity, cryptocurrency and data analytics.

**Andrew B. Whinston** is the Hugh Roy Collen Chair professor of Information Systems in the IROM department of McCombs School of Business at University of Texas at Austin. He has published several hundred papers in academic journals in Information Systems, Economics and Operations Research. He has over 130 students that have received Ph.D. degrees under his supervision. His current research area is Information Security and Related Privacy and Digital Currencies.