A Brief Blockchain Literature Review

Talley Amir
Yale University
talley.amir@yale.edu

Abstract

As our world becomes increasingly dependent on technology, more and more of our assets are being digitized - currency is no exception. Paper cash is being replaced with online and mobile banking. In the last few decades, cryptographically secure digital cash has been investigated, and more recently, decentralized blockchain-based cryptocurrencies have been explored and implemented. This technology is not only revolutionizing our transactions, but is being applied to use cases in regulatory compliance, smart contracting, and health care. This paper summarizes a few of the major advancments in blockchain technology and discusses its applications and potential extensions. This work aims to provide a brief survey of the evolution of blockchain in recent years and an overview of the present landscape of this field of research.

1 Introduction

Blockchain was first introduced in Satoshi Nakamoto's 2008 Bitcoin paper (Nakamoto, 2009) as an electronic cash system. The paper contributed a peer-to-peer transaction system that could support payments between users without going through a centralized, trusted third-party. Prior to Nakamoto's work, online payment systems relied on these trusted third-parties to ensure that payments could not be reversed. In these traditional models, when disputes between transactors arise, the centralized system (a bank) remediates the problem. Nakamoto proposed that we can achieve the same functionality by placing our trust in cryptography instead of in these third-parties and offered a practical solution: Bitcoin. This concept has since been used to implement many other types of cryptocurrencies and even extended to various other applications.

Though Nakamoto's Bitcoin technology recast the online transaction system, the design has some very severe flaws. The proof-of-work based security model that buoys Bitcoin causes high transaction latency and requires massive energy consumption. It also encourages miners to come together in order to pool their resources and mount a *51% attack*. This is an attack where more than half of the system's computing power is governed by a single adversarial group, which means that theoretically it could overturn any transaction at will. Furthermore, the pseudonymous consensus scheme supports untraceable digital criminal activity. For this reason, Bitcoin gained much attraction early on in its deployment from the Silk Road, sometimes called "Ebay for drugs" (Barratt, 2012).

In spite of these shortcomings, Bitcoin has completely reinvented the digital payment paradigm. The invention of blockchain has proven that we can perform trusted computations among mutually-distrustful parties both securely and on a large scale. Blockchain can change the way we buy, sell, invest, compute, and trust. For these reasons and many more, blockchain is a core area of research today.

2 Outline

Section 3 begins with an overview of applications of blockchain in cryptocurrencies. It also evaluates how implementations of these cryptocurrencies compare with electronic cash systems. Section 4 introduces additional applications of blockchain and details the advantages and limitations of blockchains within these contexts. Section 5 covers motivations for users to convert their wealth to digital currency, as well as motivations for miners to participate in the actual protocols. Section 6 concludes this paper with a discussion of the open problems in this area and suggestions for future research.

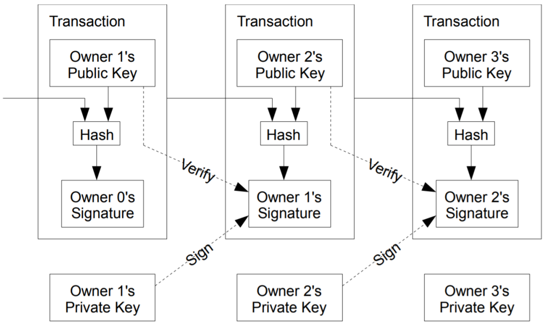

Figure 1: Bitcoin transaction flow from Nakamoto's original whitepaper (Nakamoto, 2009).

3 Blockchain & Digital Currency

Blockchain was originally devised as a solution for sending and receiving payments in the absence of trusted third-parties. In other words, it was built for *cryptocurrencies*. This section details the original blueprints for blockchain and illustrates how later works expanded on this design to enhance efficiency, scalability, and security.

3.1 Bitcoin: The Birth of Blockchain

In the Bitcoin model, a coin is "a chain of digital signatures" (Nakamoto, 2009). In order to transfer a coin from its owner to a recipient, the owner must digitally sign a hash of the previous transaction containing the coin and the public key of the recipient with the owner's private key, as shown in Figure 1. This means that anyone who can view the public ledger on which these transactions are posted can also verify the entire history of the chain of transactions.

The problem with this publicly-verifiable chain of transactions on its own is that it does not prevent a user from spending the same coin twice, which is called a *double-spending attack*. In order to protect against such attacks, Bitcoin uses a proof-of-work (PoW) based security model. In order to add a block of transactions to the ledger, a user must determine the nonce that makes the hash of the entire block (consisting of the hash of the previous block, a set of transactions, and the nonce) start with a fixed number of leading zeros. Figure 2 illustrates the components of this computation. The difficulty of finding this nonce is exponential in the number of zeros. Thus a user, in this context known as a miner, that determines this nonce first can add the transaction block to the ledger.

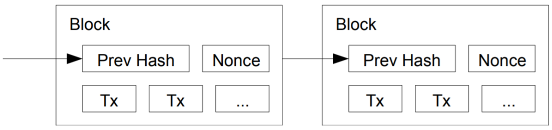

Figure 2: Schematic of Bitcoin blocks from Nakamoto's original whitepaper (Nakamoto, 2009).

In order to reverse this computation (i.e. replace it with another block of transactions which possibly even conflict with the transactions in the original block), another miner must perform the same nonce computation on its new block and extend the chain containing its block further than the chain containing the original block. This becomes much harder as more and more blocks are added to the chain with the original block. The computational infeasibility of reversing transactions on the blockchain are what give this technology its immutability, allowing its users to trust that their transactions are both correct and non-repudiable.

3.2 Scaling Consensus

With the rise in Bitcoin's popularity, many others have leveraged the same blockchain technology to construct a decentralized virtual currency. Many more cryptocurrencies have since been invented and even deployed. As a consequence, the efficiency and scalability of these systems has become of great interest to those developing them.

One mechanism that has been developed to achieve scalability in blockchain is *sharding*. This is a technique that divides the miners participating in the blockchain computation into "shards," smaller groups of miners. Miners within a shard are responsible for maintaining a portion of the ledger, and for obtaining the information necessary to validate a new transaction within their shard from other shards, when needed.

RapidChain, authored by Zamani et al. in 2018, combines sharding with a novel secure gossiping mechanism that allows shards to transfer information internally and request information from other shards quickly and with very low communication overhead (Zamani et al., 2018). This minimizes the transaction latency period and increases throughput. OmniLedger, written in 2018 just prior to RapidChain by Kokoris-Kogias et al., is another cryptocurrency that also uses sharding to achieve greater scalability (Kokoris-Kogias et al., 2018). However, this work achieves decentralized consensus via an atomic commit protocol that predefines input and output shards. Though this allows the security analysis to clearly demonstrate the correctness of the resulting transaction, the authors do not specify how the client determines a priori which shards have the information needed to verify the legitimacy of the proposed transaction. Conversely, RapidChain enables transactions to be executed without the user needing to know which shards hold what information because the nodes within the shards are equipped to retrieve the information they need to carry out the transaction. Additionally, RapidChain accomodates up to one-third fraction of corrupted nodes, whereas OmniLedger allows for only up to one-fourth.

Another interesting concept proposed in OmniLedger is an optional trust-but-verify validation mechanism. This is a process by which "optimistic" miners quickly verify small transactions in real-time. Subsequently, core validators verify and finalize the transactions, penalizing adversarial nodes whose misbehavior is detected. Since these transactions are smaller, it is not in the adversary's best interest to tamper with lower-value transactions, thereby making it less risky to process these transactions faster and with weaker security guarantees.

Other works strive to achieve scalability without sharding. Algorand, for example, uses *cryptographic sortition* to select a subset of users to run a secure Byzantine fault tolerant consensus algorithm (Gilad et al., 2017). This achieves scalability because the sortition algorithm guarantees that with high probability, the fraction of power held by the adversary in the selected committee is bounded by the same proportion as in the whole system. As a result, the consensus algorithm that approves of a proposed block of transactions maintains the same correctness guarantees as when all users in the system run the protocol. Because the algorithm's time complexity scales based on the number of users running the protocol, running with fewer users cuts the run-time substantially. Thus the size of the committee that runs the consensus algorithm can be tuned according to the desired level of security as well as the known estimated fraction of corrupted parties to achieve greater scalability.

One noteworthy similarity between sharding and sortition is that they both rely on proof-of-stake (PoS) rather than PoW. PoS is a security model in which a miner's *wealth* is used to dictate how much control that miner has in the protocol, rather than a miner's computing power as in PoW. Future works may wish to investigate whether PoW based systems can achieve as competitive a degree of scalability.

3.3 Anonymous Payments

Scaling these systems is crucial to allowing blockchain-based cryptocurrencies to be deployed and practical for widescale use. However, besides practicality in terms of efficiency, these systems also need to comply with governmental policies. In particular, blockchains should permit users to achieve some degree of privacy without jeopardizing auditability.

Zerocash proposes an anonymous payment protocol that operates in conjunction with a distributed ledger (Sasson et al., 2014). Zerocash hides not only the sender and recipient identities, but also the amount of money being transmitted. Still all payments are publicly verifiable due to *zero-knowledge Succinct Non-interactive ARguments of Knowledge* (zk-SNARKs). This cryptographic tool consists of key generation, prove, and verify algorithms. It can prove an NP statement (i.e. containment of an instance in a language) without interaction with the prover and without revealing the witness to the statement. In this context, the statement may be some variant of "I know the serial number and private key associated with some coin, thereby making it mine." Once proof of ownership of a coin is accepted, the owner of the coin can spend it. In Zerocash, double-spending is prevented by posting all serial numbers of previously spent coins publicly. After a coin is spent, it is issued a new serial number which is then only learned by the new recipient of the coin.

The option to remain completely anonymous using Zerocash is extremely appealing and far more reasonable to expect of a more widely used cryptocurrency. However, because this system is decentralized and permissionless, any user can join this system under any pseudonym and perform transactions anonymously. This is exactly the kind of dangerous setup that led to the massive rise in popularity of trading on the dark web in the early years of Bitcoin. Zerocash does have "trapdoors" that allow users to yield their private keys for the purpose of auditing and regulatory compliance, but the releasing of this information is in the hands of the user. Therefore, if someone wants to remain anonymous on Zerocash, they very easily may do so.

If blockchain systems are eventually going to be adopted worldwide, research in this area will have to develop a way for a decentralized system to be auditable and regulatable. At the very least, this technology should support some degree of access control so that under appropriate circumstances, parts of an anonymized blockchain can be recovered. At the same time, it is pertinent that regulatory compliance does not detract from the anonymity and privacy features guaranteed by the system to honest and law-abiding users.

3.4 Blockchain-less Digital Currency

While blockchain gets most of the hype, there are many more alternatives to traditional online payment models. For instance, electronic cash (ecash) was first conceived by David Chaum in 1982 (Chaum, 1982). This concept was meant to parallel cash but exist strictly virtually. Similar to real cash, ecash is "withdrawn" from a centralized authority such as a bank, but then it can be spent and circulated untraceably. To illustrate, let us briefly analyze the scheme put forth by Camenisch et al. in 2005 (Camenisch et al., 2005). This paper gives a construction for a purely cryptographic form of currency that is untraceable once withdrawn and is provably secure. It prevents double spending attacks by embedding a user's secret key into spending transactions. As a consequence, if a user spends the same coin twice, there is an efficient computation that can be performed in order to obtain the offender's secret key and gain access to all of their coins - the cryptographic equivalent of dropping your wallet on the street.

Of course ecash does not have the same decentralized structure as blockchain, which is one of blockchain's foremost selling points. Nonetheless, blockchain is not the only decentralized model. In 2018, Boyen and Haines published Graphchain, a proof of concept for a blockchain-free decentralized public ledger (Boyen, 2018). This model uses controlled depletion of fees to cause cross-verification of blocks to form a long, thin network of transactions. Though still in the early stages of development, this proposed solution claims to have security guarantees on par with Bitcoin, but may allow transactions to be processed more quickly because the blocks are no longer dependent on the entire history of a linear chain.

4 Other Applications

Though the history of blockchain is rooted in cryptocurrency, this powerful technology has found its way into solutions for problems in many other use cases. This section presents a few of these applications.

4.1 Smart Contracts

Similar to Bitcoin, Ethereum uses a blockchain to host its service (Wood et al., 2014). However, instead of transacting cryptocurrency, Ethereum allows users to host and execute *smart contracts*. Such contracts can be used to transfer money, as well as store files and other data. Using a blockchain in this manner means that one's private data is not being entrusted in some third-party, but rather in a secure decentralized network. This may be beneficial in scenarios where the information being handled would increase in value or credibility from being publicly verifiable, such as a public contract. However, other purposes that call for confidentiality may be less suitable for a platform like Ethereum.

4.2 Health Care

Blockchain can also be used to protect data in healthcare, as discussed more thoroughly in Mettler's article (Mettler, 2016). Some organizations are trying to use blockchain to ensure the integrity of drugs and detect counterfeits. The *Counterfeit Medicines Project* from *Hyperledger* aims to tackle exactly this issue. The project uses blockchain to track the chain of ownership of a drug from the point of manufacture to the time it reaches the patient. This makes tracing the path of the drug easy to do from publicly available information, thereby giving the drug its integrity.

Others are striving to use blockchains to help track patient data. A blockchain can be used to immutably store a patient's health records, automatically transfer data from wearables like fitness trackers to the blockchain, and instantly share this information with primary healthcare physicians. All data is owned by the patient, so the patient can opt to share their data with researchers for compensation. Naturally, there are questions of ethics that arise in this use case. Can and should insurance companies be able to gain access to this information? To what extent would users be able to modify their own information on the blockchain? The design and execution of blockchain systems in healthcare will not only need to consider issues of security, efficiency, and policy, but also of more nuanced issues concerning morality.

5 Motivating Participation

Many applications benefit from blockchain technology, including digital payment systems, health-tracking devices, and more. However, what does blockchain provide that other solutions do not?

One of the main advantages of blockchain is the central reason for its invention: Decentralization. Blockchain does not rely on trusting third-parties to validate a computation performed among two entities, whether this be a payment, a smart contract, or a permanent digital record. The trust in the correctness and non-repudiability of these systems is guaranteed by the infeasibility of certain computations, which means that users need not trust a person – they need only trust cryptography.

Conversely, there are many reasons *not* to use blockchain. In most of these blockchain based systems, users are pseudonymous, which means that transaction flows can be used to track a user's spending. Zerocash is one system that has anonymity and privacy guarantees, but there is still the ethical issue of regulating these systems. What policies are needed in order to avoid a another scandal like the Silk Road? With complete anonymity, it is extremely difficult to audit these systems. Even more difficult is to audit only parts of the system for criminal activity without compromising the privacy of honest users. Finding a way to make anonymity finer-grained without reverting back to a centralized model is a problem of these systems that remains unsolved.

Beyond blockchain's technical difficulties, there is the concern of energy consumption. Enormous computing power is needed to implement and sustain a cryptocurrency, especially in PoW models. As of 2019, Bitcoin accounts for 0.26% of global electricity consumption (Dig, 2019). Over time this may affect the profitability and appeal of mining for Bitcoin as well as other PoW based distributed ledgers, ultimately causing these systems to collapse.

In light of these challenges, blockchains need to motivate users to partake in their protocol such that users somehow gain something in exchange for their participation. The Byzantine, Altruistic, Rational (BAR) adversarial model aims to account for this concern. Under the BAR assumption, there are a bounded number of adversarial agents, and the remaining users are some combination of altruistic agents (users that strictly adhere to the prescribed protocol) and rational agents (users that are true to the protocol unless it benefits them to deviate).

One example of a blockchained system that is proposed and analyzed under the BAR assumption is YODA (Das et al., 2018). This paper proposes a protocol for executing computationally intensive smart contracts off-chain in a secure way. The analysis shows that rational agents do not deviate from the protocol because the underlying system is based on proof-of-stake. Thus if a user does deviate from the protocol, they lose the stake they invested in order to participate. If instead the user behaves honestly, they are rewarded for contributing to the computation in the prescribed protocol.

The BAR model encompasses both Byzantine and rational behavior, making it a more realistic setting for analyzing the security of blockchains. Other works predating the BAR model may benefit from considering how they perform when assessed within this model. Further research should also ascertain to what extent evaluations within this model carry over to empirical observations in security post-deployment.

6 The Future of Blockchain

Though far from comprehensive, this paper demonstrates that there are many considerations to be made when developing a blockchain-based system. Different designs have their uniquely desirable features, each one aiming to strike a balance among many competing factors such as scalability, profitability, anonymity, auditability, efficiency, integrity, and so on. There is no one-size-fits-all blockchain solution. Rather, blockchain is a malleable tool that can be tailored to cater to its users' needs. As the applications of blockchain become even further diversified, more complex considerations will need to be integrated into future blockchain solutions.

Acknowledgments

I would like to thank Mariana Raykova for advising me throughout my writing of this paper.

References

2019. Bitcoin energy consumption index.

Monica J. Barratt. 2012. Silk road: Ebay for drugs. *Addiction*, 107(3):683–683.

Christopher. Haines Thomas Boyen, Xavier. Carr. 2018. Graphchain: a blockchain-free scalable decentralised ledger. pages 21–33.

Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. 2005. Compact e-cash. Cryptology ePrint Archive, Report 2005/060. `https://eprint.iacr.org/2005/060`.

David Chaum. 1982. Blind signatures for untraceable payments. pages 199–203.

Sourav Das, Vinay Joseph Ribeiro, and Abhijeet Anand. 2018. YODA: enabling computationally intensive contracts on blockchains with byzantine and selfish nodes. *CoRR*, abs/1811.03265.

Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. 2017. Algorand: Scaling byzantine agreements for cryptocurrencies. In *SOSP*.

E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford. 2018. Omniledger: A secure, scale-out, decentralized ledger via sharding. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 583–598.

M. Mettler. 2016. Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–3.

Satoshi Nakamoto. 2009. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com*.

E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. 2014. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459–474.

Gavin Wood et al. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151:1–32.

Mahdi Zamani, Mahnush Movahedi, and Mariana Raykova. 2018. Rapidchain: Scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, pages 931–948, New York, NY, USA. ACM.