Maintaining Scalability in Blockchain

Anova Ajay Pandey[1], Terrance Frederick Fernandez[2][0000-0002-7317-3362], Rohit Bansal[3], Amit Kumar Tyagi[1,4] [0000-0003-2657-8700]

[1]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai

[2]Department of Information Technology, Dhanalakshmi Srinivasan College of Engineering and Technology, Chennai

[3]Department of Management Studies, Vaish College of Engineering, Rohtak

[4]Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, Tamilnadu, India

anovaajay.pandey2019@vitstudent.ac.in, frederick@pec.edu, rohitbansal.mba@gmail.com, amitkrtyagi025@gmail.com

Abstract. The history of cryptocurrencies like Bitcoin and Litecoin and even the meme coins like Dogecoin have developed fast. Blockchain, the technology that underpins these digital currencies, has drawn considerable interest from the academic community and the business community, including on Twitter. Aside from security and privacy, the blockchain has several other advantages. The average time it takes for a transaction to be validated and stored in each peer node so that it cannot be reversed or revoked is used to measure the performance of blockchain networks. Even though this is referred to as "throughput," it should not be confused with the number of transactions processed at any given time.

To put it another way, the ability of a blockchain network to handle more transactions and more nodes is called scalability. Yet, scalability is problematic to reach a more robust platform of users and transaction load. We will focus on scalability issues and ways to maintain them efficiently. We will also go through the research challenges and future work for blockchain. Hence, researchers working on blockchain have aimed for a lower level of scalability to let the network's throughput grow sub-linearly because the size of the network increases. The resulting schemes are mostly mentioned as scale-out blockchains. We have heard of Sharding, Lightning Network or Ethereum Plasma and Matic; they all will be considered as scale-out solutions to the matter of blockchain scalability.

Keywords–Blockchain; Ethereum; Bitcoin; Scalability; Decentralisation; Sharding; DApps

1. Introduction

Crypto-currencies with underlying technology as blockchain has gained their light in these recent years. Some emerging and significant industries are applying the technology into many areas, for example, IoT and smart cities. Blockchain has many plus points like decentralization, security, anonymity, and democracy. More attention garnered a lot of on-chain activity, however as we've seen within the past few months, fees become costly. The confirmation time of dealing will increase once Ethereum approaches the limit of ~15 transactions per second (tps). Prices that are too high make it more difficult for people to use Ether (ETH) as an easy payment or run Decentralized Apps (DApps), some of which can only operate at a high level if the fees are kept low. As the chain grows in size, problems with decentralization will arise. As hardware requirements for running an Ethereum full node rise, the network's ability to spread will be hampered, and adoption will be more difficult. Few people will try to set up a node if it takes too long or requires expensive equipment.

It's worth noting that ETH fees are paid in units called gas, which is ETH's free currency. A simple payment would be required to pay less gas than a complex sensible contract because the latter requires a lot of computation. The higher the gas value, the more likely a transaction will be confirmed more quickly. The transparency of the blockchain is because all transactions are publicly accessible. To recognize or identify the person, we keep track of transactions using anonymous public addresses and hide the nodes' identities from the real world to locate them.

Because the network's nodes make all of the decisions, it is transparent and easy to find the sources of any errors. Automated transaction generation, data storage, and decision-making are all possible with Smart contracts. Scalability is the main reason why blockchain isn't being used as a generic platform for a variety of applications and services. With a maximum throughput of 14 transactions per second, Ethereum outperforms Bitcoin, the first blockchain-based cryptocurrency to be discovered, which can only handle about 3-4 transactions per second on average. By distributing the execution of consensus algorithms across multiple nodes, consistency is preserved. Integrity, confidentiality, and authorization are the three pillars upon which the security of a blockchain system is built.

The trilemma of maintaining Decentralisation, Scalability, and Security (Refer Figure 1) is still there but maintaining scalability is the main criteria of this paper.

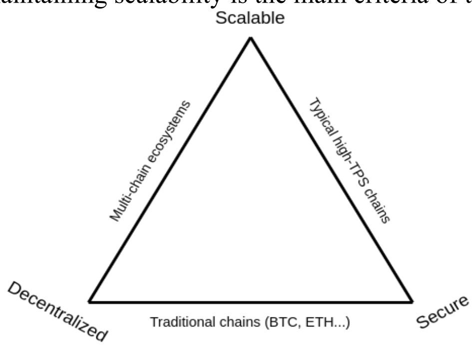

Figure 1: The Scalability Trilemma

Organization of work:

- Section 2 discusses Literature Survey

- Section 3 discusses the methodology to be used for a more Scalable blockchain.
- Section 4 discusses proposed solutions like incentivization and punishments for secure and decentralized chains.
- Section 5 discusses the Results for various Scaling solutions.
- Section 6 discusses the Conclusion and Future work for scalability and other techniques discussed in this paper and References.

2. Literature Survey

We have three main aspects of scalability, throughput, storage, and networking. Many start-ups are coming with solutions for this issue, like Polygon Matic, Cardano, and others. In the trilemma mentioned earlier, we can only choose at most two out of the three. The same goes with these three, throughput, storage, and networking. If we focus on only improving scalability, we need to compromise with the other two. We can use different combinations of them whenever we need to in an application. We already have existing technologies or solutions for scalable blockchain systems.

Current scalability issues:
One by one, we will discuss Storage, Throughput, and Networking.

Throughput:
Throughput refers to the number of items moving through a system or process. The number of transactions per block and the time between blocks impact the throughput of blockchain systems. The throughput of blockchain, for example, is seven transactions per second. Contrast this with the current VISA system, which can process an average of 2000 transactions per second. The block interval is 10 minutes for a Bitcoin blockchain system, and the transaction volume is limited to one megabyte. As a result, we must devise precise schemes to boost throughput.

Storage:
Various devices that users use generate large amounts of data when blockchain is applied to real-world business situations. A node must store complete transactions back to the genesis block in the current Blockchain system or algorithm. Using blockchain in real-world settings is challenging because nodes have limited storage and processing power. The safekeeping of such a large amount of data on a distributed ledger should be investigated and a matter of concern.

Networking:
The scalability of blockchain systems is affected by this factor. Each node in the current blockchain system has a limited number of resources. Due to the need for network bandwidth, this mode of transmission cannot be scaled up to handle many transactions. Block propagation delays are exacerbated when nodes are informed of a transaction update twice. As a result, finding a better way to transmit data is critical.

3. Methodology

All three terms can be broken down into two categories: throughput, which is the number of transactions per block and the time between blocks, and storage, which refers to data storage. These technologies, which will be discussed below, are ways to increase and understand scalabilities.

Increasing the block size:
It's possible to increase the block size to boost throughput, which will also increase throughput simultaneously. To process and confirm transactions, some nodes must work harder.

By reducing the size of transactions:
Reduce transaction size by increasing the number of transactions in each block. 60-70 percent of all transactions are authenticated by digital signatures used to verify their authenticity. Digital signatures are segregated from the rest of the transaction data and are pushed to the end of the blocks by SegWit. As a result, the transaction size is reduced, and each block contains a more significant number of transactions. To put it another way, if we do so, the amount of data in a single block will increase.

Reduce the number of transactions processed by nodes:
Decoupling control and management from execution via off-chain transactions is one of the three solutions.

Off-chain Transactions:
Off-chain transactions are those that take place on a cryptocurrency network outside of the blockchain. There is a growing interest in off-chain transactions, particularly among prominent participants, due to their low or no cost. Transactions that require multiple signatures can be processed more quickly by creating off-chain micropayment channels. The Lightning Network and the duplex Micropayment Channels are examples of off-chain transactions that are still processed on the blockchain; they are vastly different in many ways. The Lightning Network sends a small amount of data to the blockchain every time a micropayment channel is updated.

Anatomical updates of initial funds are more likely to support Duplex Micropayment channels than other micropayment channels.

Sharding:
Sharding is a technique for distributing an extensive data set across a flat surface; it is a notice in software engineering. Every shard represents a tiny fraction of the total transaction. Creating new chains, referred to as "shards," will reduce network congestion and increase the number of exchanges per second (Refer Figure 3). Other than flexibility, this is significant. Running an agreement calculation on a large number of businesses helps sharded hubs agree. The throughput of sharded blockchain frameworks increases linearly as more seats are added. Some examples of sharding blockchain frameworks include Plasma and Polkadot.

The Matic Organization is currently employing plasma. Using a square maker layer to generate blocks solves the problem of helpless exchange execution in Matic Organization. The framework can produce blocks at a fast rate, thanks to the square maker. Decentralization is ensured through the use of PoS designated spots shipped off the main Ethereum chain. Two hundred sixteen exchanges on an uneven chain are thus possible for Matic.

Decoupling The executives/Control from Execution:
The prerequisite of value and administration and applications by decoupling the board/control and executing brilliant agreements as codes should be possible through virtualization. Dissimilar to most existing DLT frameworks that don't recognize various administrations and applications, DLT expressly considers different administrations' QoS prerequisites. In particular, administrations and applications are arranged into multiple classes reliable with their QoS prerequisites, including affirmation inertness, throughput, cost, security, protection, and so on. This is a change in perspective from the current blockchain-situated DLT frameworks to cutting-edge administration arranged DLT frameworks.

Empowering innovations identified with block time frame:
Exchange serialization implies that the chosen pioneer hubs approve exchanges and create new squares. To limit impacts in pioneer political decisions, the pioneer hubs are chosen like clockwork. In customary blockchain frameworks, every pioneer political decision can produce a substitution block. To lessen the square time framework on the throughput, moderate pioneer political race and quick exchange serialization must be decoupled. Numerous advancements have embraced the thought into three classifications as per their chief political race components. Fixed Pioneers: Hyperledger texture assigned a selected bunch of pioneer hubs that run the PBFT agreement convention to approve exchanges and settle on new squares. Small squares contain dialogues and are created by the chosen pioneer at a quick rate.

Between two key impedes, the chosen pioneer can produce different miniature squares.
Aggregate Pioneers: to diminish the affirmation season of the blockchain framework, change the pioneer's political decision to be a board of trustee's political decision. A gathering of pioneers is chosen to approve exchanges and affirm blocks to keep up with the framework's decentralization. Byzantine agreement calculations empower quick exchange affirmation; others delegate the approval of the business**.** On the board, individuals' democratic force corresponds to the quantity of their agreement bunch shares. In this manner, the board of trustees' individuals in ByzCoin are progressively changed. When a hub discovers a PoW arrangement, the reconfiguration occasion is set off. The panel then, at that point, concludes if to add the new part. Whenever added, then the most established part is taken out from the advisory group**.**

Advancements for information stockpiling:
Dispersed frameworks and existing information stockpiling are combined with increasing capacity. They were using Circulates Hash Tables, the power (DHT). Off-

chain DHT is used to store the raw data, while the blockchain is used to keep only the information references. References to the information are SHA-256 hashes. DHT and IPFS will be integrated with blockchain as part of a larger plan to address the capacity challenge. Off-chain stockpiling arrangements can hold a lot of data, but they are not as durable as on-chain stockpiling arrangements. The blockchain hubs cannot straightforwardly handle the off-chain information. Furthermore, arrangements for off-chain capacity complicate exchange checks. While verifying transactions, blockchain hubs had the opportunity to request information from the off-chain stockpiling frameworks about the transactions that had occurred.

Innovations for Information Transmission:
Sending all the information about the exchange occurred and diminished the prerequisite for the organization to transfer speed assets, here we examine a couple of innovations and their proposed answers for this issue. RINA: Cardano (chips away at Ethereum based framework) embraces Recursive Between Organization Engineering, another innovation to scatter exchange data. RINA gives a secure and programmable climate to proliferate information effectively. Fiber: it's the fast square transfer network for the Bitcoin Blockchain framework. There are immediately six Fiber hubs, disseminated deliberately throughout the earth. Excavators can accompany Fiber hubs to both send and receive blocks in the model of the middle-and-talked model. They are reducing the amount of data the blockchain organization has to deal with.

It may be possible to reduce the amount of information that is disseminated by only exchanging information once. As a general rule, it's hoped to take advantage of the fact that blockchain hubs all have access to the same exchange data. Blocks like Xtreme Thin are like conservative squares. To transmit exchange hashes, the Sprout Channel employs an additional numerical strategy. Hubs can use Blossom Channels to decide whether or not missing exchanges in other hubs' memory pools should be addressed. When a square is generated, the missing deals are developed in addition to the square header and, therefore, the hashes of discussions.

4. Proposed Solutions and Techniques to further develop Versatility

A viable strategy for improving throughput can be to decouple pioneer political decisions and exchange serialization. All the blocks are produced rapidly by chosen pioneers utilizing Byzantine agreement conventions adds the suspicion that what 33% of the hubs are flawed. At the same time, the remainder of them executes effectively. Some blockchain frameworks select pioneers hooked into the calculation escalated PoW, which isn't a proficient energy methodology and burns-through plenty of power as a force.

Motivators and discipline instruments:
Hubs are self-intrigued; therefore, the motivator instruments are essential to propel hubs to contribute their endeavors to see the information. Some excavators check the knowledge and execute the exchange. Mining is the way toward making new bitcoin by settling a computational riddle. It's essential to stay up with the record of trades

after that a cryptographic money like bitcoin is predicated. Diggers have gotten extremely refined within the foremost recent entirely while utilizing complex hardware to accelerate mining tasks. Two strategies for motivating force and discipline instruments, exchange expenses and money issuance, are two standard techniques. Considering the Bitcoin blockchain framework, when an excavator effectively produces a square, it acquires 6.25 new bitcoins.

Portions of monetary standards and exchange charges among these pioneers should be planned fastidiously. To forestall twofold spending assaults and rebuff malevolent pioneers, discipline instruments need to be embraced. Affirmation time is often utilized as a strategy. The motivations could also be given within the wake of investing the affirmation energy. Within the event that any invalid or twofold spending exchange is recognized, there'll be no motivators given or moved. This instrument is critical as a reasonable measure of the store will be a prize for the diggers and a discipline or a misfortune for the pernicious assailants. Keeping a high standard of motivating force may prompt centralization because it would be unreasonable to the pioneer to form new squares. Subsequently, appropriate planning of the impetuses is going to be beneficial and safe.

Consensus and verification:

Speed of consensus is also a factor in how well a blockchain system works. The difficulty of a PoW block only rises as the number of transactions increases, implying that it will take longer and require more resources to process a transaction. In addition, it's important to note that PoW is unsustainable. These solutions are necessary because they can address the issue of scaling without increasing block sizes or introducing other measures that may interfere with the technology's capacity for decentralization and high levels of security without increasing block sizes or introducing other measures. Layer 1 blockchain solutions help to reinforce rock-bottom protocols, such as Bitcoin's PoW, which changed the way they work in data processing.

When it comes to a consensus algorithm, Ethereum is currently using proof of stake (PoS). Using this new mining method allows for faster transactions and better utilization of energy. Another layer one scaling solution discussed above is sharding, which breaks down authenticating and validating transactions into smaller pieces. For the first time, a more comprehensive range of nodes can participate in a peer-to-peer network (P2P). Block execution can be sped up by all of these. Blockchains can be scaled in more ways than just through Layer 1 solutions. An additional protocol built on top of blockchains such as Ethereum and Bitcoin is necessary for layer two scaling solutions to work.

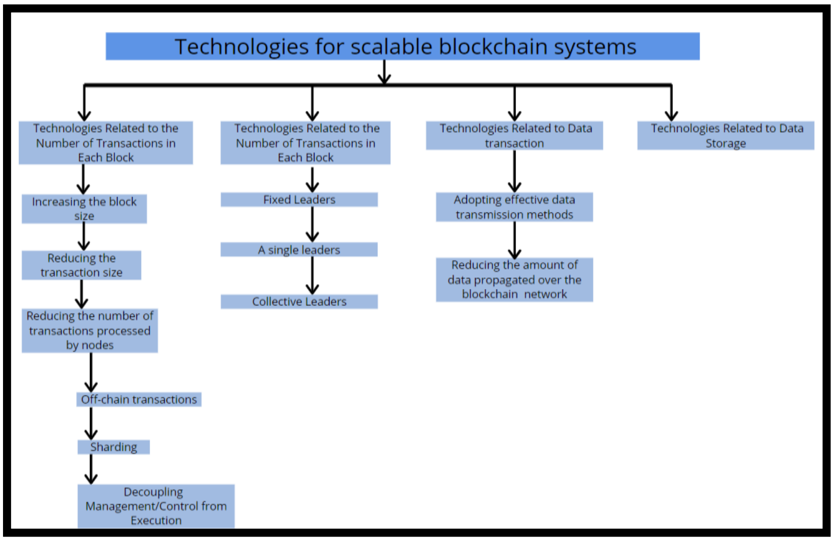

Figure 2: Division of Technologies related to Maintaining and Improving scalability

The core decentralization and security features of the core blockchain can be maintained with layer two scaling solutions. If you've heard of Ethereum 2.0, you've probably heard of a PoS-based system with support for fragmentation and other scalability features that are intended to replace the Ethereum network. The scalability of Ethereum will improve due to these changes, allowing it to compete with other leading blockchains. Ethereum investors who put money into the platform can earn rewards by staking their coins in return for their validation efforts.

5. Results for improvising scaling in blockchain

As a separate blockchain linked to the Ethereum main net, Plasma Chain can use proofs against fraud to arbitrate disputes such as Optimistic rollups. These chains are often called "child" chains because they are essentially smaller versions of the Ethereum main net. Chains of Merkel trees can be infinitely stacked on top of each other, allowing for a constant bandwidth flow from the parent chains (including the main net). Each child chain has its mechanism for verifying the validity of the blocks in the parent chain. Ethereum's Plasma layer two solution employs "child" or "secondary" blockchains to help confirm the chain. In many ways, plasma chains are similar to Polka dot’s smart contracts. To release the work and improve scalability, they're organized in a hierarchical structure.

Scaling blockchain:
It is possible to scale the base layer by uploading or sharing your work to a second level. For most transactions, Layer 1 serves as the primary consensus layer. Only intelligent contracts are needed for layer 2, which is built on top of layer one and does not require any changes to layer 1. The base layer can handle 15 transactions per second, but layer two scalings can increase that to 2000 to 4000 per second. Ethereum

developers are currently working on Ethereum 2.0, which uses proof of stake and sharding to improve transaction throughput on the base layer. To handle more transactions in the future, we will need layer two scalings. It is clear from Figure 2 that scaling blockchain-based systems is possible.

Scalability cannot be sacrificed for the sake of security and decentralization. Increasing the capabilities of layer two scalings, like transaction speed and throughput, improves off-chain capabilities. It's a great way to save money on gas. Channels are one of the most widely discussed scaling solutions, and some solutions are payment-specific. Channels allow users to perform multiple transactions and only submit two transactions to the base layer. State channels and their subtype Payment channels are the most popular, but they do not allow open participation. It is necessary for users to be known and for multi-sig contracts to be in place to secure their funds. Lightning's network makes extensive use of payment channels.

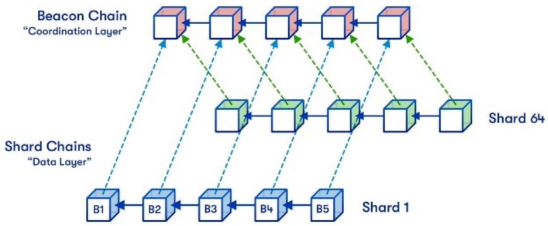

Figure 3: Sharding Example

Joseph Poon and Vitalik Buterin proposed plasma, an Ethereum development framework. Smart contracts and Merkel trees in plasma have no upper limit on the number of child chains created. By offloading transactions from the leading chains, transactions can be quickly and cheaply transferred between child chains. Layer 2 of Plasma requires a longer wait time before funds can be withdrawn. Plasma or channels cannot be used to scale general-purpose intelligent contracts. It makes use of Plasma Side-chains and the Proof-of-Stake network to deliver Ethereum transactions that are scalable, quick, and secure. A modified version of the Plasma framework is employed.
"Side-chains" are blockchains with their consensus models and block parameters compatible with Ethereum. Because of this, side-chain contracts and Ethereum-based contracts can be deployed to the Ethereum virtual machine simultaneously. A side chain can take many forms. XDY is just one of many.

Rollups:
A cryptographic verification, a snark compact non-intelligent contention of information, is created and submitted to the base layer to maintain and improve scaling. Rollups handle all exchange states and execution within chains. Most of the Ethereum chain is simply a means for storing and exchanging data. Optimistic and ZK rollups are the two main types of rollups. Bright Rollups are slower, but ZK Rollups are faster and more effective. Idealistic rollups do not provide a primary path to the overall intelligent agreements to move to layer two. Virtual machines run by

Idealistic Rollups are called "OVM," or "Optimistic" virtual machines because they consider the execution of intelligent agreements frequently carried out on Ethereum.

It makes overall keen agreements easier and faster to deal with their composability, which is highly relevant in decentralized money where all significant sensitive arrangements were at that battle. It is important. Good faith, which is getting closer and closer to the central net dispatch, is probably the most critical task performed on idealistic rollups. When ZK is included, this is when Decentralized trades based on layer 2 have rollups and broadens. Then there's ZK sync, which makes it possible to use crypto payments more flexibly. Ethereum 2.0 also has the potential to enhance adaptability. Scalability of the information layer is all that is required for rollups. Ethereum 2.0 stage 1, which deals with information sharding, will give them an incredible boost. Regardless of the availability of a variety of layer two setups.

It appears that the Ethereum community is unified in its approach to scaling through rollups, and Ethereum 2.0 stage 1 information sharding was also confirmed. A new post by Vitalik Buterin called a rollup-driven Ethereum guide. There are many ways to scale decentralized money so that it is more accessible to the general public.

6. Conclusion and Future work

Blockchain technology's various benefits will attract organizations and businesses worldwide without a doubt to take a position more ahead of what it is now. It is still in its initial phase, but this, one of the most recent technologies, will take a much longer time to gain our identity, which requires patience. The rise of Ethereum and the various possibilities that we could do with blockchain. It allowed intelligent contracts, making it possible to have much more complex use cases than Bitcoin and for computer programs to be built and executed on the blockchain. However, the pros of blockchain are hard to ignore. Still, the technology will help various industries because the verification for each piece of knowledge that goes in and through these Blockchain systems will prevent the many adversities.

This will continue to be a topic of discussion shortly as blockchain technology is adopted and used in a wide range of applications. The performance of Blockchain 3.0 networks has dramatically improved, but they have yet to be widely adopted. When looking for a high-performance blockchain platform that can handle thousands of transactions per second, let's make sure that the use case we're looking for is compatible with it first.

Acknowledgment
The authors want to thank the Centre for Advanced Data Science and School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, for providing their kind support to complete this research work on time.

References

[1] Florian Tschorsch, Björn Scheuermann, Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, IEEE Communication Surveys & Tutorials, Vol. 18, NO. 3, 2016.

[2] Yonatan Sompolinsky, Aviv Zohar, Accelerating Bitcoin's Transaction Processing Fast Money Grows on Trees, Not Chains, International Association for Cryptologic Research, 2013.
[3] IttayEyal, AdemEfeGencer, EminGünSirer, and Robbert van Renesse, Bitcoin-NG: A Scalable Blockchain Protocol, USENIX The Advanced Computing Systems Association, 2016.
[4] Rhett Creighton, Domus Tower Blockchain, Domus Tower Inc. (DRAFT), 2016
[5] Bellare, M., and Rogaway, P., Random oracles are practical: A paradigm for designing efficient protocols, In Proceedings of the 1st ACM conference on Computer and communications security,1993
[6] Bitcoin community, Bitcoin source, https://github.com/bitcoin/bitcoin, Mar. 2015.
[7] Eyal, I., Birman, K., and van Renesse, R., Cache serializability: Reducing inconsistency in edge transactions,35th IEEE International Conference on Distributed Computing Systems, ICDCS, 2015
[8] Bitcoin community, Protocol rules, https://en.bitcoin.it/wiki/Protocol_rules, Sep. 2013.
[9] Marko Vukolic, The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, IBM Research – Zurich, 2015
[10] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012):28, 2008.
[11] I. F. Blake and P. Gadiel Seroussi Nigel Smart, Advances in Elliptic Curve Cryptography, vol. 317. Cambridge, U.K.: Cambridge Univ. Press, 2005
[12] Marko Vukolic, The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, IBM Research – Zurich, 2015
[13] Miller, A., and Jansen, R. Shadow, Bitcoin: Scalable simulation via direct execution of multithreaded applications, IACR Cryptology ePrint Archive, 2015.
[14] Miller, A., and Jr., L. J. J., Anonymous Byzantine consensus from moderately-hard puzzles: A model for Bitcoin. https://socrates1024.s3.amazonaws.com/consensus.pdf, 2009.
[15] Sompolinsky, Y., and Zohar, A., Secure high-rate transaction processing in Bitcoin, Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, 2015
[16] Florian Tschorsch, Björn Scheuermann, Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, IEEE Communication Surveys & Tutorials, Vol. 18, NO. 3, 2016.
[17] G. Wood. Ethereum: A secure decentralized transaction ledger. http://gavwood.com/paper.pdf
[18] B. Kreuter, B. Mood, A. Shelat, and K. Butler. PCF: A portable circuit format for scalable two-party secure computation. In Security, 2013
[19] IttayEyal, AdemEfeGencer, EminGünSirer, and Robbert van Renesse, Bitcoin-NG: A Scalable Blockchain Protocol, USENIX The Advanced Computing Systems Association, 2016.
[20] Miller and J. J. LaViola Jr. Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin, 2014.
[21] Marko Vukolic, The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, IBM Research – Zurich, 2015

[22] Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013a. URL {http://ethereum.org/ethereum.html}.
[23] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In 12th Annual International Cryptology Conference, pages 139–147, 1992.