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

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

[2]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, rohitbansal.mba@gmail.com, frederick@pec.edu, amitkrtyagi025@gmail.com

Abstract. In the history of cryptocurrencies like Bitcoin and Litecoin and even the meme coins like the Doge coin have developed really fast. These digital currencies work on the basis of blockchain, it has gained great attention from twitter, academia and Industry. Block chain has many features like transparency, anonymity, democracy, decentralization and security. The performance of blockchain networks is usually measured because the average time it takes for a transaction to be validated and stored in each peer node during a way that it can't be reversed or revoked. While this is known as throughput, it shouldn't be misinterpreted with the number of concurrent transactions processed during a given frame of time. Scalability of blockchain networks is that the ability of the platform to support increasing the load of transactions, also as increasing the number of nodes within the network. Yet there is a problem with scalability to reach a greater platform of users and transaction load. We will focus on scalability issues, and ways to maintain it 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 throughput of the network grow sub-linearly because the size of the network increases. The resulting schemes are mostly mentioned as scale-out blockchains. We have definitely 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 its light in these recent years. Some emerging and major industries are applying the technology into many areas for example IoT and smart cities. Blockchain has many plus points like Decentralisation, 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 and also the confirmation time of a dealing will increase once Ethereum approaches the limit of ~15 transactions per second (tps). Larger fees increase the prices for folks exploitation Ether (ETH) as an easy payment or maybe Decentralized Apps (DApps), a number of which can solely operate at associate degree best level with lower fees. There are issues for decentralization if the chain grows large, hardware necessities to run associate degree Ethereum full node over time will increase considerably, reducing spreading and raising the barrier to adoption. If it takes too long to line up a node or need costly hardware, then few folks are going to be incentivized to try to do so.

Ethereum fees are unit measured in units called gas, that is freelance of the crypto asset ETH. an easy payment would be needed to pay a lower quantity of gas than a sophisticated sensible contract, since it needs a lot of computation for the latter. Users may choose a high gas value to extend the possibilities of obtaining their transactions confirmed faster. Blockchain gives everyone access to all transaction records, which makes it transparent. We can recognise or identify the person by keeping track of transactions using public anonymous addresses and keeping the identities of the nodes, hidden from the real world.

All the decisions are made by the nodes in the network, this makes it transparent and fault can be caught easily. A piece of code or code known as Smart contracts have the ability to generate transactions, data storage and decision making automatically. The main issue why blockchain is not being used as a generic platform for different applications and services is due to scalability. Bitcoin, the first known blockchain-based cryptocurrency, can perform only an average of about 3-4 transactions per second while Ethereum improves the throughput to about 14 transactions per second, which is still not much capable to deal with high frequency transactions scenarios. Consistency is maintained by running the consensus algorithms among decentralized nodes. Security of a blockchain system depends on three important keys, integrity, confidentiality and authorization.

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

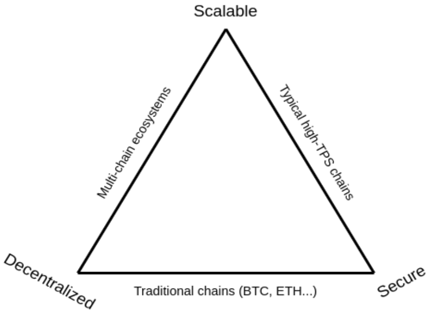

Figure 1: The Scalability Trilemma

Organisation of work:

- Section 2 discusses Literature Survey
- Section 3 discusses Methodologyto be used for more Scalable blockchain.
- Section4discussesProposed solutions like incentivization and punishments for secure and decentralized chains.
- Section 5discusses the Results for various Scaling solutions.
- Section 6discusses 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. The trilemma which was mentioned earlier, we can basically only choose at most two out of the three. 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 issues with scalability:
One by one we will discuss Storage, Throughput and Networking.

Throughput:
Items passing through a system or in a process is known as throughput. The throughput of blockchain systems is related to the number of transactions in each block and block interval time. In blockchain if we talk about throughput for example blockchain, it is 7 transactions per second. Compared to the current system of VISA which can handle 2000 transactions per second on an average. The block interval time for a Bitcoin blockchain system is 10 minutes, and the number of transactions is narrowed to one megabyte. Hence we need to design accurate schemes to increase the throughput.

Storage:

When we apply blockchain to real business terms, large quantities of data are generated by various devices used by the users. In the current Blockchain system or algorithm used, each node must store complete transactions back to the genesis block. It is difficult to apply blockchain to real environments where nodes have only a limited storage and computing resources. Storing this much amount of data in blockchain that to with available resources effectively should be studied and be a topic of concern too.

Networking:

One of the factors that affect the scalability of blockchain systems. The blockchain system which we currently use is a broadcast medium in which each node with limited resource. This mode of transmission cannot be scaled upto handle a plenty oftransactions due to requirement for network bandwidth resources.Also sending the nodes about the update of the transaction twice increases the block propagation delay. That is why it is important to create a more efficient way of data transmission.

3. Methodology

If we analyze all these three terms, we understand that throughput is the number of transactions in every block and the block interval time; generating data comes under the term storage and transmission of data is related to networking.

These technologies which will be discussed below are ways to increase and understand scalabilities.

Increasing the block size:

To increase the throughput we can increase the block size, but that will also increase throughput hand in hand. Some nodes need to work more to process and confirm transactions.

By reducing the size of transaction:

Increasing the number of transactions in each block is to reduce the transaction size. Digital signatures are used to verify the authentication of transactions, accounting for 60-70 percent of the transactions size. Segregated Witness, also known as SegWit, separates digital signatures from the rest of the transaction data and pushes the digital signatures to the end of the blocks. In this way, the transaction size is reduced and one block contains more transactions. That means if we do so, one block can contain more transactions.

Reduce number of transactions processed by nodes:

Off-chain transactions, sharding and decoupling control/management from execution are the three solutions.

Off-chain Transactions:

The transactions occurring on a cryptocurrency network which move the value outside of the blockchain. Due to their no or low cost, off-chain transactions are gaining attention, especially among large participants. The basic idea of off-chain transactions is that if nodes make frequent transactions, off-chain micropayment channels are created between nodes to handle the multi-signature transactions off chain instantaneously. The final settlement transactions are processed on the blockchain Lightning Network and duplex Micropayment Channels are two implementations of off-chain transactions. There is a main difference between them. The Lightning Network needs to commit some information to the blockchain for each update of the micropayment channels.

If we compare both of them the Duplex Micropayment channels often support the anatomical update of initial funds over the channels off the blockchain.

Sharding:

Sharding is the way toward parting a data set on a level plane to spread the heap; it's a typical idea in software engineering. Every shard measures a little part of all the exchange. It will diminish network clog and increment exchanges each second by making new chains, known as "shards" (Refer Figure 3). This is significant for reasons beside adaptability. Hubs inside a shard concur on a bunch of exchanges by running an agreement calculation. In sharding blockchain frameworks, the throughput increments straightly as more hubs join the frameworks.

Plasma and Polkadot are a portion of the instances of sharding blockchain frameworks.

Plasma is at present being utilized by the Matic Organization.Matic Organization takes care of the issue of helpless exchange execution by utilizing a square maker layer to create blocks. The square maker permits the framework to create blocks at an extremely quick rate. The framework utilizes PoS designated spots shipped off the primary Ethereum chain to guarantee decentralization. This permits Matic to hypothetically carry out 2^{16} exchanges on an uneven chain.

Decoupling The executives/Control from Execution:

The prerequisite of value and administration and applications by decoupling the board/control and the execution of brilliant agreements as codes should be possible through virtualization. Dissimilar to most existing DLT frameworks that don't recognize various administrations and applications, vDLT expressly considers the QoS prerequisites of different administrations and applications. In particular, administrations and applications are arranged into various 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 just produce a substitution block. To lessen the square time frame work on the throughput, moderate pioneer political race and quick exchange serialization ought to be decoupled. The thought has been embraced by numerous advancements into three classifications as per their chief political race components. Fixed Pioneers: Hyperledger texture assigned a fixed bunch of pioneer hubs that run the PBFT agreement convention to approve exchanges and settle on new squares.Miniature squares contain exchanges 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 pioneers political decision to be board of trustees political decision. A gathering of pioneers are chosen to approve exchanges and affirm blocks for keeping up with decentralization in the framework. Byzantine agreement calculations empower quick exchange affirmation, others delegate the approval of the exchange**.** In the board, individuals' democratic force is corresponding 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 board 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:
For capacity we join existing information stockpiling with the dispersed stockpiling frameworks. The capacity utilizing Circulates Hash Table (DHT). The crude information is put away off chain DHT, while holding just the information references on the blockchain. The references are the SHA-256 hashes of the information. The overall plan to address the capacity challenge is to join blockchain with existing dispersed stockpiling frameworks, like DHT and IPFS. Off-chain stockpiling arrangements can store a lot of information, yet penance permanence. The blockchain hubs can't handle the change of the off-chain information straightforwardly. In addition, off chain capacity arrangements likewise make exchange check more perplexing. While confirming exchanges, blockchain hubs had the opportunity to demand chronicled exchange information from the off-chain stockpiling frameworks.

Innovations for Information Transmission:
Sending all the information about the exchange occurred and diminish 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 Bitcoin Blockchain framework. There are immediately six Fiber hubs, disseminated deliberately all throughout the earth. In sight of the middle-and-talked model, excavators can accompany Fiber hubs to send and obtain blocks. Diminishing the measure of data cover the blockchain organization.

Spreading every exchange on just one occasion may be a successful method to diminish the measure of proliferated information. The general thought is to take advantage of the way that blockchain hubs have comparable exchange information in their memory pools. Xtreme Thinblocks is like Conservative Squares. because of the fundamental distinction it utilizes an additional numerical strategy called the Sprout Channel to impart exchange hashes. Hubs can utilize Blossom Channels to make a decision about the missing exchanges in other hubs' memory pools. At the purpose when a square is produced, notwithstanding the square header and therefore the hashes of exchanges, the missing exchanges are additionally engendered.

4. Proposed Solutions and Techniques to further develop Versatility

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

Motivators and discipline instruments:

Hubs are self-intrigued therefore the motivator instruments are important to propel hubs to contribute their endeavors to see information. There are excavators who check the knowledge and execute the exchange. Mining is the way toward making new bitcoin by settling a computational riddle. it's important to stay up with the record of exchanges whereupon a cryptographic money like bitcoin is predicated. Diggers have gotten extremely refined within the course of the foremost recent quite while utilizing complex hardware to accelerate mining tasks. Two strategies for motivating force and discipline instruments, exchange expenses and money issuance are two normal techniques. Considering the Bitcoin blockchain framework, when an excavator effectively produces a square, it acquires 6.25 new bitcoins as of now.

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 are 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 an inexpensive measure of store are going to be a prize for the diggers and a discipline or a misfortune for the pernicious assailants. Keeping a high measure of motivating force may prompt centralization because it would be exorbitant to the pioneer to form new squares. Subsequently appropriate planning of the impetuses are going to be beneficial and safe.

Consesus and verification:

The speed of reaching a consensus will also affect the performance of the blockchain system. Proof of labor (PoW) involves tons of computation, and therefore the block difficulty only gets higher with scale, which suggests longer and resources to process a transaction. And to not mention that PoW is unsustainable. Solutions for scaling are necessary as they can tackle the issues by providing breaks or time-outs for the blockchain without having the need to increase block sizes or introduce other measures which may tamper with the technology's capacity for decentralization and high levels of security. Layer 1 blockchain solutions help to reinforce rock bottom protocols for E.g.: Bitcoin's PoW, which changed the way they work in data processing.

As an example, the Ethereum network is now moving to a proof-of-stake (PoS) consensus algorithm. This new mining method supports quicker transactions and more efficient use of energy in the mining process. Sharding as discussed above is another layer 1 scaling solution that helps break down the work of authenticating and validating transactions into smaller pieces. It spreads the workload better across the peer-to-peer (P2P) network to inaugurate more computing power from more nodes. All of these can achieve faster block execution. Layer 1 solutions aren't the sole avenue available to scale blockchains. Layer 2 solutions to scaling establish an extra protocol that's built on top of blockchains like those of Ethereum and Bitcoin.

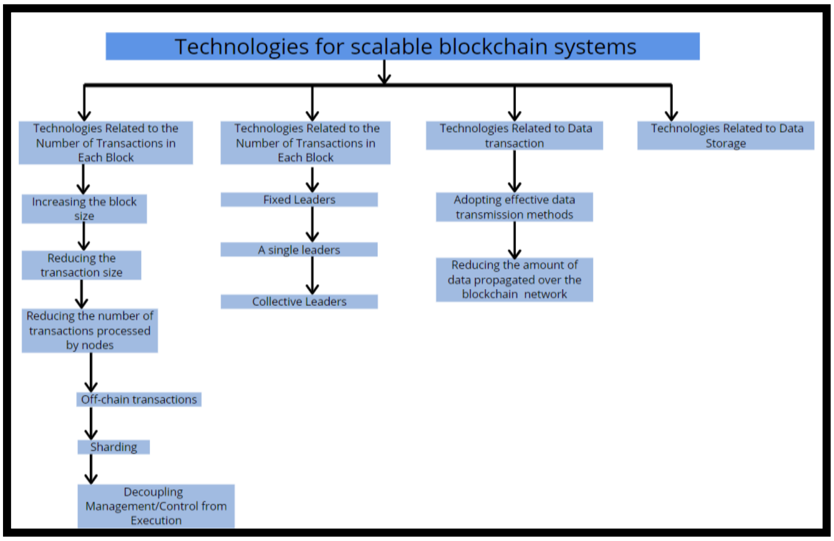
Technologies for scalable blockchain systems
Technologies Related to the Number of Transactions in Each Block
Increasing the block size
Reducing the transaction size
Reducing the number of transactions processed by nodes
Off-chain transactions
Sharding
Decoupling Management/Control from Execution
Technologies Related to the Number of Transactions in Each Block
Fixed Leaders
A single leaders
Collective Leaders
Technologies Related to Data transaction
Adopting effective data transmission methods
Reducing the amount of data propagated over the blockchain network
Technologies Related to Data Storage

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

Layer 2 scaling solutions can improve performance without changing the core decentralization or security features that are an integral part of the core blockchain.

Ethereum 2.0 refers to the transition from the Ethereum network to a more flexible PoS-based system that supports fragmentation and other scalability features. These series of improvements will improve the scalability of Ethereum and take it on a level equal to other leading blockchains in terms of performance. Investors investing in Ethereum can stake their coins to earn rewards in return to their contribution to validation efforts.

5. Results for improvising Scaling in blockchain

Plasma Chain can also be a separate blockchain, linked to foremost Ethereum and then uses the proofs against fraud for Eg. Optimistic rollups to arbitrate disputes. These chains are sometimes mentioned as "child" chains as they're essentially smaller copies of the Ethereum mainnet. Merkel trees enable creation of a limitless stack of those chains which will work to dump bandwidth from the parent chains (including mainnet). These derive their security through fraud proofs, and every child chain has its own mechanism for block validation. Child or secondary blockchains are used in Ethereum's Plasma layer 2 solution which will assist the chain in verification. Plasma chains are almost like smart contracts from Polkadot. They are structured in a hierarchy, differently to require transactions from the main chain to release the work and upgrade scalability.

Scaling blockchain:
Scaling the base layer or Scaling the layer by uploading or sharing some of the work to another layer, layer 2. Layer 1 is our standard base consensus layer, where pretty much all transactions are settled. Layer 2 is built on top of layer 1 it doesn't require any changes in layer 1, only needs smart contracts, layer 2 increases 15 transactions on base layer can be conducted, but layer 2 scaling can dramatically increase transactions upto 2000 to 4000 transactions per second. Ethereum developers are working on Ethereum 2.0 which works with proof of stake and sharding, which will also gradually increase the transaction throughput on the base layer itself. We do require layer 2 scaling for it to be able to handle a higher number of transactions in future. Figure 2 depicts a clear picture or provide technologies for Scaling blockchain based systems.

Security and Decentralization cannot be compromised as a cost of Scalability. Layer 2 scaling helps increase the capabilities off chain like transaction speed and throughput. It can greatly reduce gas fees. Some solutions are payment specific, most popular scaling solutions, channels are one of the widely discussed solutions. Channels enable the users to execute their transactions a number of times, and only submit two transactions to the base layer. State channels and its subtype Payment channels, are the most popular types of channels they do not offer open participation, they are application specific. Users have to be known and have multi-sig contracts in which their funds will be locked up. The concept of payment channels are greatly used by bitcoin's lightning-network.

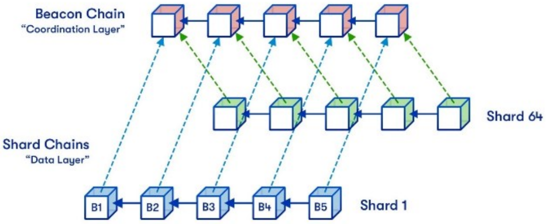

Figure 3: Sharding Example

Joseph Poon and Vitalik Buterin proposed a framework named Plasma, for building scalable applications on Ethereum. Plasma takes advantage of the utilization of smart contracts and Merkel trees to create an infinite number of child chains, copies of parent chains. Offloading transactions from the chains into child chains allows for quick and affordable transactions. Plasma has a drawback, the users need to wait for longer period of time if they want to withdraw the funds from layer 2. Plasma as well as channels, cannot be used to scale general purpose smart contracts.Matic uses a Matic Network, which provides scalable, faster and secured Ethereum transactions using Plasma Side chains and a Proof-of-Stake network. It uses an adapted version of plasma framework.

Side chains are Ethereum compatible independent blockchains, with their own consensus models and block parameters interoperability with Ethereum is made possible by using the same Ethereum virtual machine so contracts deployed to the Ethereum based layer, can be deployed directly to the side chain. XDY is one example of one such a side chain.

Rollups:

They maintain and improve scaling by packaging or moving up into one exchange and creating a cryptographic verification additionally alluded to as a snark compact non-intelligent contention of information, just this confirmation is submitted to the base layer. With rollups all exchange state and execution are taken care of inside chains. the most Ethereum chain, just stores exchange information. There are two kinds of rollups, ZK Rollups and Optimistic Rollups. ZK rollups are quicker and more effective than Optimistic Rollups. Idealistic Roll Ups don't give a basic way to the overall shrewd agreements to relocate to layer 2. Idealistic Rollups run an EVM viable virtual machine called OVM, Optimistic virtual machine which takes into account executing the shrewd agreements that are frequently executed on Ethereum.

In light of the fact that it makes it simpler and quicker for the overall keen agreements to deal with their composability which is incredibly pertinent in decentralized money where all significant keen agreements were at that point fought. Probably the most task performing on idealistic rollups is good faith which is drawing nearer and nearer to the principle net dispatch. At the point when it includes ZK Rollups and broadens are acceptable examples of decentralized trades based on layer 2. On top of that we've ZK sync empowering adaptable crypto installments. Adaptability likewise can be amplified by Ethereum 2.0. Rollups just need the information layer to be scaled. they will get an inconceivable lift effectively in Ethereum 2.0 stage 1 which is about the sharding of information. Notwithstanding a range of layer 2 arrangements accessible.

It is very much like the Ethereum people group is on the uniting approach of chiefly scaling through rollups, And Ethereum 2.0 stage 1 information sharding was likewise affirmed. during a new post by Vitalik Buterin, called a rollup driven Ethereum guide. This load of scaling arrangements can make decentralized money more open to everybody.

6. Conclusion and Future work

Blockchain technology's various benefits will attract organizations and businesses round the world without a doubt to take a position more ahead of what it is now. It is still in its initial phase but this, one among the most recent technologies will take a much longer time to gain its identity amongst us, and this requires patience. The rise of Ethereum and the various possibilities that we could do with blockchain. It allowed for smart contracts, which made 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, but the technology will indeed help various industries because the verification for each piece of knowledge that goes in and through these Blockchain systems are going to be a preventor of the many adversities.

Blockchain performance and scalability will still be a subject of intrigue within the near future as blockchain technology is adopted and applied for a spread of use cases. there's a big performance improvement in Blockchain 3.0 networks, though they're yet to ascertain wide scale adoption. But before we start our search journey for a high performing blockchain platform that supports thousands of transactions per second, allow us to be doubly sure on whether the utilization case that the answer is being envisaged requires an equivalent.

Acknowledgment
The authors want to thank 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 In 12th Annual International Cryptology Conference, pages 139–147, 1992.