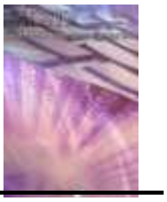
DSR Design for Scientific RENAISSANCE



THE SCALABILITY CHALLENGE OF THE BLOCKCHAIN: A REVIEW

Musharaf Unissa Rahiman[1], Imad Fakhri Al Shaikhli[2], Fardous Mohamed Eljadi[3]
Department of Computer Science. International Islamic University of Malaysia[1,2], Department of Computer Science
Faculty of ScienceUniversity of Tripoli, Libya[3]

ISSN (Printed): 2314-7350
ISSN (Online): 2231-8852

Abstract- The blockchain is an equivalently new innovation utilized for storing and verifying transaction records for online cryptocurrencies like Bitcoin. The framework is expandable and distributed, making it hard for transactions to be rehashed, copied, or faked. During the transaction process many unsolved issues have been noticed such as there is no data privacy as many blockchains are public and scalability. Scalability is an important concern to ensure large-scale adoption of blockchain systems. The throughput of a blockchain is limited if it grows linearly and peers are forced to execute transactions serially. This paper aims to provide an overview which outlines on the major challenge of the blockchain which is the scalability issue. Moreover, in order to assist the development process of new technologies the pros and cons of previous techniques used for improving the scalability challenges of the blockchain are summarised.

Keywords- Blockchain, challenges, scalability, transactions, techniques.

1. INTRODUCTION

Blockchain was recently established and introduced in the epoch of technology bringing a new method to security, resiliency and productiveness for the systems. Although originally made obtainable by bitcoin, blockchain is much more than an outset for cryptocurrency. It provides a protected way to trade any kind of excellent service or transactions [1]. Blockchain technology was originated in 2008 to record bitcoin [2] transactions in an unalterable and publicly dependable way. Bitcoin was the first paradigm of cryptocurrency and was invented to authenticate money transfers between parties without relying on any moderator [3]. Though blockchain technology is often analyzed as possibly tough in various situations, there is a lack of insight where and how blockchain technology is strongly applicable and where it has uncommon experimental effects [4]. In public blockchain any person can be part of the nodes and make contributions to achieve the rewards by following up the laws.

The absolute previously known case of blockchain technology appeared in November 2008 in a whitepaper titled 'Bitcoin: A Peer to Peer Electronic Cash System' composed by a certain individual – or gathering of people – working under the pseudonym Satoshi Nakamoto [2]. Even though not known much about the inventor, Nakamoto's whitepaper would proceed to shape the establishments of the Bitcoin peer-to-peer digital currency, introduced a little week later as an open source venture in January 2009. Bitcoin was one of a kind in that it empowered people to transact legitimately with each other, without the requirement of a confided tertiary mediator (like a bank or clearing house) to encourage their transactions.

This paper has been organized in a specific manner. Section 2 is made up of literature review regarding the blockchain and scalability, and some existing techniques which were used earlier are discussed. For better understanding the pros and cons of those techniques are described in a table.
After that, the paper discusses the reviewed constructions and concludes with future work.

2. LITERATURE REVIEW

Blockchain has defined to have many advantages like decentralization, persistency, anonymity and auditability. As a growing technology, various challenges and issues is being faced by blockchains [5]. More and more researchers realize that the blockchain can be removed out from the digital currency to create a revolutionary technical architecture in other areas [6]. Some researchers have started to study the hidden technologies such as the difficulty in the scalability of consensus algorithms [7] and the smart contract [8].

Bitcoin depends on proof of work mining to protect consensus which is complex, mining requires an enormous expense on energy, confirmation of transactions which is slow, and security is difficult to quantify [4]. One reason why it is impractical to utilize a blockchain immediately is a direct result of the poor performance. Public blockchains, where anybody can take part, can process only a few transactions for every second and is subsequently a long way from usable in the realm of finance.

Permissioned blockchains is another kind of blockchain where just a few authorized users reserve the options to choose what will be recorded in the blockchain. This permits permissioned blockchains to have many advantages over public blockchains. Most quiet is the capability to part the system into fragments where just a subset of nodes needs to approve transactions to a particular application, permitting the utilization of parallel computing and better scaling. Besides, the approving nodes can be trusted, permitting the utilization of consensus algorithm which offer considerably more throughput [9].

As the transaction level has expanded, the blockchain has turned out to be heavier and the capacity dimension of Bitcoin blockchain has surpassed 100GB. Each transaction made should be put away for its approval. As the capacity limit of storage is restricted numerous little transactions are deferred and miners charge those transactions of high transaction fee. Additionally, the huge block size will diminish the speed and prompts blockchain branches for this situation scalability issue is exceptionally very tough [5].

Scalability

Scalability is a connection of several frameworks and metrics. It is also a problem to correlate one factor to the huge array of factors that might affect performance and scalability adhesively [10]. Highly limited scalability is one of the main problem with Satoshi’s blockchain [11]. Scalability can be analyzed and measured with several metrics involved [10]. The bitcoin scalability issue alludes to the study with respect to the limitations on the measure of transactions the bitcoin network works on. It’s connected to the way that records (known as blocks) in the bitcoin blockchain are constrained in size and frequency [12].

The on-chain transaction handling limit of the bitcoin system is constrained by the normal blocks creation time of 10 minutes and the block size limit. These together oblige the network's throughput. The transaction preparing limit most extreme is assessed between in the range of 3.3 and 7 exchanges for each second [11]. Bitcoin has turned into a great example of overcoming adversity, in spite of its consensus latencies on the order of an hour and the theoretical peak throughput of just up to 7 exchanges for every second. The circumstance today is profoundly unique and the poor execution scalability of early POW blockchains makes sense anymore [7].

Techniques Used For Improving the Scalability Issue of the Blockchain

Given the absence of scalability premises of existing blockchains, a couple of ongoing works have proposed to shard the blockchain so as to build the achieved scalability and throughput of the framework [13]. Hyperledger Fabric is said to be surely a lot quicker and scalable than both Bitcoin and Ethereum, and it can guarantee information access to permit just the member in involved with a transaction can see sensitive information. In spite of the fact that the inquiry still stands if Hyperledger Fabric is quick and scalable enough to supplant the incorporated frameworks utilized today [9].

The MAST (Merkelized Abstract Syntax Tree) is a proposed strategy in Bitcoin's BIP-114, which joins Merkle Tree and Abstract Syntax Tree. Merkle Tree is a paired tree, it is a way to deal with recursively repeat to interface two hashes of each transaction of a block, and thereupon hash the two hashed transaction yet again and associate them until they become one. Abstract Syntax Tree is a way to deal with interface every limit until all the connections of the program are joined together [15].

Methodologies like IOTA, SegWit or the Lightning Network attempt to comprehend the scalability issues of blockchain applications. In [16] its mentioned that unfortunately, they center around procedures backing off the blockchains development as opposed to lessening the issues emerging from a developing chain or acquaint new ideas to out the linear blockchain altogether.

Segwit is a patch designed to secure transaction malleability. As described in (Wright, 2017) [17] SegWit opens the chance to present sidechains. These are less secure than on block scaling, yet for what it's worth yet to be tested, there can be just expectation that they will be adequate. The issue is that it is not verified, and it isn't sufficient. The primary issue originates from shortage, the second concerns the genuine scalability of the framework.

ELASTICO was proposed by [18] for open blockchains. This Sharding protocol divides the mining network into small groups where the transactions shards are processed in parallel. As analyzed by the researcher in Elastico's is generally little shards (e.g.100 validators per shard in investigations) yield a high dissatisfaction probability of 2.76% 1 for every shard for each block under a 25% enemy, which can't safely be free in a POW framework [18]. For 16 shards, the disappointment probability is 97% over only 6 epochs. Second, Elastico's shard determination isn't unequivocally inclination safe, as miners can specifically dispose of POWs to predisposition outcome [19].

Third, Elastico does not guarantee transaction atomicity across shards, leaving assets in a single shard bolted perpetually if another shard rejects the transaction. Fourth, the validators always switch shards, compelling themselves to store the worldwide state, which can ruin execution yet gives more grounded certifications against adaptive adversaries [20].

OmniLedger, a novel scale-out distributed record referenced [20] preserves long term security under permissionless activity. It guarantees security and rightness by utilizing a predisposition safe public-randomness protocol for picking huge, measurably delegate shards that process transactions, and by presenting a productive cross shard commit protocol that automatically handles transactions influencing numerous shards.

GHOST was implemented and a variant of it was added as part of the Ethereum project, a second-generation distributed applications platform. Instead of the longest branch scheme, GHOST weighs the branches and miners could choose the better one to follow [21]. SPECTRE [22] enjoys both high throughput and fast confirmation times. It uses the structure of the DAG to represent an abstract vote concerning the order between each pair of blocks. One caution of SPECTRE is that the output of this pairwise ordering may not be extendable to a full linear ordering, due to possible Condorcet cycles [11].

The main idea behind SPECTRE is a voting algorithm referring to the order between each pair of blocks in the DAG. The voters are blocks (not miners); the vote of each block is executed algorithmically (and not provided interactively) according to its location within the DAG [21]. The Phantom introduced in 2018 as mentioned in [11] is a protocol for transaction confirmation that is secure under any throughput that the network can support.

Table 1. List Of Techniques Used Previously For Improving Scalability Issues Of The Blockchain

TECHNIQUES FOR IMPROVING SCALABILITY	DESCRIPTION	PROS	CONS
Big block	• Big Block is just an approach to expand the limited block size.	• Trans mission limit is huge. • The cost of transmission is cheaper.	• As the block size expands engendering speed turns out to be moderate bringing about fork event as often as possible.
MAST (Merkelized Abstract Syntax Tree)	• MAST is a method of making Bitcoin script into a merkle tree.	• Privacy is high as one branch is hidden so as the information is not known.	• As the another branch is not hidden privacy is completely not guaranteed.
Segwit (Segregated Witness)	• It's the method by which the block size limit on blockchain is increased by deleting signature data from Bitcoin transactions.	• Possibility to apply different solutions to Bitcoin.	• It makes the code complex and prompts fungibility issues.
Sharding	• It's a strategy where nodes are assembled shaping a shard and makes every shard to form various blocks.	• This decrease the weight on the every node, and it can improve throughput by parallel processing transactions.	• When attackers have unlimited authority over any single shard, the data trustworthiness is broken, which means 1%

			attack.
Lightening Network	• To be safely routed over various distributed payment channels which enables the usage of proposed Hashed Timelock Contracts (HTLCs).	• It can decrease the transaction charge and backup time and decrease the weight on the primary chain.	• As the transaction charge vanishes, the benefits of the minors fall, so the biological systems of them may change.
Segwit (Segregated Witness)	• It's the method by which the block size limit on blockchain is increased by deleting signature data from Bitcoin transactions.	• Possibility to apply different solutions to Bitcoin.	• It makes the code complex and prompts fungibility issues.
Plasma	• Series of contracts which runs on top of a root blockchain.	• It has tree structure of parent-child blockchain.	• The verification process is expensive.
Atomic-swap	• Aims to trade resources between various blockchains.	• It can package various blockchains and trade resources between them.	• Both blockchains must utilize a similar algorithm dependent on Pow, a hash-competing algorithm.
Omni-Ledger	• It is a novel scale-out distributed record referenced preserves long term security under permissionless activity.	• Ensure S security what's more, accuracy by utilizing an inclination safe public-randomness protocol.	• As the real throughput is reliant on the remaining task at hand then the framework is better with just a single shard.
GHOST	• It's a method for fighting the manner in which that quick block time blockchains experiences the ill effects of a high number of stale blocks.	• Finding genuine fundamental chain to create all blocks or all block headers.	• Still inclined to few attacks, for example, it uncovers the framework to DOS assaults.

SPECTRE	• It's a protocol for the consensus core of cryptocurrencies that stays secure even under high throughput & quick confirmation times.	• It's a voting algorithm alluding to the order between each pair of blocks.	• The pairwise requesting may not be extendable to a full linear ordering.
PHANTOM	• A protocol for transaction affirmation that is secure under any throughput that the network can support.	• It utilizes a Directed Acyclic Graph of blocks, otherwise known as blockDAG, a hypothesis of Satoshi's chain which better suits a setup of fast or huge blocks.	• The waiting time is more when conflicts are visible.

3. DISCUSSIONS

The techniques mentioned above which were used for improving the blockchain scalability issues is been discussed and compared as follows.

The scalability technique Big Block as mentioned in [17] states how the speed decreases and results in fork when the block size increases. MAST (Merkelized Abstract Syntax Tree) is a technique where the privacy is hidden and not guaranteed and on the other side PLASMA has its verification process expensive. Another implementation of Sharding mentioned in [23] describes that when attackers have complete control over any single shard, the data trustworthiness is broken, and attacks takes place.

The recent technique PHANTOM introduced in the year 2018 as mentioned in decreases and results in fork when the block size increases. MAST (Merkelized Abstract [11] uses a blockDAG which is more suitable to setup huge blocks but still there is a problem within itself where the waiting time becomes more when there are conflicts which still has to be taken care of [24]. The recent techniques mentioned above still have their drawbacks which is yet to be improved for the blocks to be efficiently scalable.

4. CONCLUSION AND FUTURE WORK

In this paper different techniques used previously in improving scalability issue are reviewed and given a brief description of each technique which were introduced in recent years. Their pros and cons are also mentioned so as to analyze that there are still drawbacks with those techniques and they still have to be improved.

The future work will be focused on bringing in a technique which is called as Hashgraph to improve scalability issue of the blockchain as the study states that still there are drawbacks faced in the scaling of the blockchain.

REFERENCES

1. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. 2017 IEEE Technology and Engineering Management Society Conference, TEMSCON 2017, (2016), 137–141. https://doi.org/10.1109/TEMSCON.2017.7998367

2. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org*, 9. https://doi.org/10.1007/s10838-008-9062-0

3. Gatteschi, V., Torino, P., Torino, P., & Torino, P. (2018). To Blockchain or Not to Blockchain: That Is the Question, (April), 62–74. https://doi.org/10.1109/MITP.2018.021921652

4. Kwon, J. (2014). TenderMint : Consensus without Mining. *The-Blockchain.Com*, *6*, 1–10. Retrieved from tendermint.com/docs/tendermint.pdf

5. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

6. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A Review on Consensus Algorithm of Blockchain. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2567–2572. https://doi.org/10.1109/SMC.2017.8123011

7. Vukolić, M. (2016). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9591, 112–125. https://doi.org/10.1007/978-3-319-39028-4_9

8. Idelberger, F., Governatori, G., Riveret, R., & Sartor, G. (2016). Evaluation of Logic - Based Smart Contracts for Blockchain Systems, 1(July), 1–17. https://doi.org/10.1007/978-3-319-21542-6

9. Scherer, M., & Eriksson, J. (2017). Performance and Scalability of Blockchain Networks and Smart Contracts, 46. https://doi.org/UMEA University.

10. Goswami, S. (2017). Scalability Analysis of Blockchains through Blockchain Simulation, (May), 67.

11. Sompolinsky, Y., Zohar, A., & Science, C. (2018). Phantom: A Scalable BlockDAG protocol. Retrieved from https://eprint.iacr.org/2018/104.pdf

12. Croman, K., Decker, C., Eyal, I., Efe Gencer, A., Juels, A., Kosba, A., Wattenhofer, R. (2016). On Scaling Decentralized Blockchains Initiative for CryptoCurrencies and Contracts (IC3). International Conference on Financial Cryptography and Data Security, 106–125. https://doi.org/10.1007/978-3-642-03549-4

13. Zhang, K., & Jacobsen, H. (2018). Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains.

14. Li, W., Sforzin, A., Fedorov, S., & Karame, G. O. (2017). Towards Scalable and Private Industrial Blockchains. Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts - BCC '17, 9–14. https://doi.org/10.1145/3055518.3055531

15. Kim, S. (2018). A Survey of Scalability Solutions on Blockchain. 2018 International Conference on Information and Communication Technology Convergence (ICTC), 1204–1207.

16. Ehmke, C., Wessling, F., & Friedrich, C. M. (2018). Proof-of-Property – A Lightweight and Scalable Blockchain Protocol, (January), 48–51.

17. Wright, C. S. (2017). The Illusion of Scale in Segregated Witness. Ssrn. https://doi.org/10.2139/ssrn.2993315

18. Luu, L., Narayanan, V., Baweja, K., Zheng, C., Gilbert, S., & Saxena, P. (2015). SCP: A Computationally-Scalable Byzantine Consensus Protocol For Blockchains. IACR Cryptology EPrint Archive 2015, 1168. Retrieved from https://www.weusecoins.com/assets/pdf/library/SCP - A Computationally-Scalable Byzantine.pdf

19. Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). Is Bitcoin a Decentralized Currency? IEEE Security and Privacy, 12(3), 54–60. https://doi.org/10.1109/MSP.2014.49

20. Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies. In Security and Privacy (SP), 2017 IEEE Symposium on (pp. 375-392). IEEE.

21. Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B. (2018). OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. Proceedings - IEEE Symposium on Security and Privacy, 2018–May, 583–598. https://doi.org/10.1109/SP.2018.000-5

22. Sompolinsky, Y., Lewenberg, Y., & Zohar, A. (2016). SPECTRE : Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections.

23. Fynn, E., & Pedone, F. (2018). Challenges and Pitfalls of Partitioning Blockchains. Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN-W 2018, 128–133. https://doi.org/10.1109/DSN-W.2018.00051

24. Ruta, M., Scioscia, F., Ieva, S., Capurso, G., & Sciascio, E. Di. (2017). Semantic Blockchain To Improve Scalability In The Internet Of Things. Open Journal of Internet of Things, 3(1), 46–61. Retrieved from http://sisinflab.poliba.it/publications/2017/RSICD17/VLIoT_VLDB2017_accepted.pd