Newer Generation Blockchain Technology Has Added Significant Runtime Performance Improvements When Compared to 1st Generation Blockchain (Bitcoin)

Robert T. Mason
(*Anderson College of Business and Computing, Regis University, Denver, CO, USA)*

Abstract: This paper discusses improvements in the runtime performance for newer generation blockchain technology. The use of private versus public Blockchain (1st generation) accounts for significant runtime performance differences. For example, Hyperledger Fabric that uses private Blockchain is scalable to support 20,000 transactions per second (tps), where as Bitcoin that is public Blockchain supports an average of 5 tps.

Keywords: Blockchain

I. INTRODUCTION

Bitcoin and the concept of blockchain was first conceptualized in a seminal paper by Satoshi Nakamoto.[1] Over the last decade, the use of blockchain has evolved from supporting digital currencies (e.g. Bitcoin, Ethereum) into a variety of industries (e.g. Healthcare, Accounting, Finance, Insurance, Agriculture). Drescher [2] defines Blockchain as:

"a purely distributed peer-to-peer system of ledgers that utilizes a software unit that consist of an algorithm, which negotiates the informational content of ordered and connected blocks of data together with cryptographic and security technologies in order to achieve and maintain its integrity."

In the area of Healthcare, Metcalf et al. [3] define blockchain as an open, decentralized technology that provides a mechanism to establish trust between participating organizations via one or more immutable (unchangeable) distributed digital ledgers. A key word in this definition is that blockchain provides a mechanism to establish "trust" between participating and often disparate organizations using one or more immutable distributed digital ledger(s).

Slow performance of the Blockchain has been a problem since its' inception in 2008.[4] This paper investigates these performance issues and provides examples of significant improvements in the performance of the Blockchain technology.

II. PRIVATE VERSUS PUBLIC BLOCKCHAIN

Bitcoin currently supports the processing on average of 5 transactions per second (tps).[5] A later generation of Blockchain technology called Hyperledger Fabric supports 3,000 tps and is scalable to 20,000 tps.[6] Therefore, this large difference in tps for the two Blockchain technologies, begs the question: Why is Hyperledger Fabric able to process so much more tps in comparison to Bitcoin? One major advantage of Hyperledger Fabric is that it is a private Blockchain versus Bitcoin that is a public Blockchain.

Public Blockchains, such as Bitcoin and Ethereum, are called permissionless blockchain platforms because they protect a user's anonymity.[7]This feature is important for digital currencies because users can buy and sell the currency without the control of third-party institutions such as large banks or the federal government. Anyone who is willing and able to install the Bitcoin blockchain software on an internet server can participate in the Bitcoin blockchain network, provided they are willing to follow the prescribed Bitcoin processes and rules. As of 2019, Bitcoin surpassed 100,000 participating nodes (servers) that comprise the Bitcoin network.[8] Because of the use of public Blockchain, an identical version of the Bitcoin software is installed on each of the participating servers across the internet. This large number of servers is useful to safeguard the integrity of the Bitcoin software and the currency transactions, from fraud and double spending.

However, a disadvantage of having a large number of nodes is that adding a new transaction block to the Bitcoin ledger is slow and time consuming. To add a new block to the Bitcoin network, a consensus of the participating servers (51%) must agree to add the new block. Bitcoin blocks have an average size of 1.4 megabytes and the Bitcoin network averages 408,622 transactions per day (which is roughly 5 tps). In this example, more than 51,000 Bitcoin servers will need to review and approve a new Bitcoin block within a network of 100,000 servers. Eventually, the block is added to the ledger that spans the 100,000 nodes and payment is made to the Bitcoin node (miner) that solved a hash puzzle and proposed the new block. This large volume of internet communication and coordination between many servers is one reason that the tps of Bitcoin is slow in comparison to a Hyperledger Fabric blockchain network.

Newer generations of Blockchain technology that are often used by businesses, use the private Blockchain (a.k.a. permissioned networks) according to Massessi.[7]All of the participating servers in a private network must be verified and approved prior to the node joining the network. Users are given access to create transactions depending upon their user profile. Private networks tend to be much smaller because they are composed of only trusted stakeholder nodes. Unlike Bitcoin, identical Blockchain software for a private network is not replicated to all participating nodes. Instead, each node has a specific job type. For example, within a Hyperledger Fabric Network, there are three different types of software on the nodes based on job type (e.g. functionality). This configuration for different job types allows for the size of the software footprint to be significantly smaller on each node, hence using less CPU and storage [9]:

1. Client or submitting-client: a client server submits the actual transaction invocation to the endorser servers (described below), and then broadcasts transaction proposals to the ordering service server.
2. Peer: a node that commits transactions and maintains a copy of the ledger and the state of the ledger. Peer servers can also have another role as a special endorser. Note: Hyperledger Fabric can have multiple public or private ledgers depending upon the configuration of the network.
3. Ordering-service-node or orderer: this server acts as a communication service that implements a delivery guarantee to notify all other servers once consensus for a block is achieved.

The ability to access the private network is important because verification allows the establishment of user permissions. Therefore, only authorized users can access the private blockchain network [7]. The permissioned approach for user access reduces the number of participating nodes and users for a private blockchain network when compared to a public Blockchain. This reduction in the number of users and nodes allows for the division of work across different node types, which reduces the amount of CPU usage and network communication that occurs between nodes.

Another major improvement for private Blockchain is the elimination of mining. As mentioned previously, Bitcoin nodes must compete with one another to be able to add new blocks to the ledger by solving complicated hash puzzles. Bitcoin servers that are able add new blocks to the public Blockchain are rewarded by earning Bitcoin. Solving hash puzzles can be a CPU and memory intensive process for Bitcoin nodes. Mining is not a requirement for private blockchain networks. The private nodes take turns adding new transaction blocks to the ledger. Therefore, this major difference in private Blockchain that excludes mining, results in less CPU and memory usage.

III. CONCLUSION

In conclusion, improvements in the runtime performance for newer generation blockchain technology (Hyperledger Fabric) are substantial when compared to 1st Generation Blockchain (Bitcoin). Private Blockchain networks have significantly improved their runtime performance by applying three major changes:

1. The division of functionality into different node types reduces the size of the software footprint and number of tasks that each private node must complete. For example, the Hyperledger Fabric Private Blockchain Network has three server types of Client, Peer and Orderer.
2. Permissioned access to the network for user access reduces the number of participating nodes for a private Blockchain network in comparison to a public Blockchain network like Bitcoin.
3. Mining (solving complex hash puzzles) that is a CPU and memory intensive process is not performed for private Blockchain networks.

REFERENCES

[1]. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. Bitcoin. https://bitcoin.org/bitcoin.pdf.

[2]. Drescher, D. Blockchain basics: a non-technical introduction in 25 steps. New York, NY: Apress, 2017. (ISBN 978-1-4842-2604-9)

[3]. Metcalf, D., Bass, J., Hopper, M., Cahana, A., and Dhillon, V. Blockchain in Healthcare: Innovations that Empower Patients, Connect Professionals and Improve Care (HIMSS Book Series). New York, NY: CRC Press, 2019. (ISBN-13: 978-0367031084)

[4]. Thakkar, P., Nathan, S. and Viswanathan B.Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform. 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Milwaukee, WI, 2018, pp. 264-276, doi: 10.1109/MASCOTS.2018.00034.

[5]. Blockchain.2020. Transaction Rate. Blockchain. https://www.blockchain.com/en/charts/transactions-per-second.html.

[6]. Gorenflo, C., Lee, S., Golab, L., Keshav, S. Fast Fabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second. arXiv (Cornell University). https://arxiv.org/pdf/1901.00910.pdf. Accessed 3 May 2020.

[7]. Massessi, D. Public Vs Private Blockchain In A Nutshell. 2018. Medium. https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f.

[8]. North, M. Bitcoin Network Surpasses 100,000 Nodes, New Data Shows, 2019. Bitcoinist. https://bitcoinist.com/bitcoin-network-surpasses-100000-nodes-new-data-shows/

[9]. Hyperledger Fabric. Architecture Origins,2020. Hyperledger Fabric. https://hyperledger-fabric.readthedocs.io/en/release-1.4/arch-deep-dive.html.