Study on Blockchain Technologies for Modern Enterprise Applications

David A. Rodríguez Pérez
Master of Engineering in Computer Engineering
Advisor: Dr. Jeffrey Duffany
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract – *We are living on a time where emerging technologies are disrupting the way we work in multiple industries. One of these technologies is distributed ledgers called Blockchains. Within the enterprise, we are analyzing and expanding the Blockchain technology implemented in a private and secure environment where only our trusted users will be able to participate and want to answer a basic question. Given the less amount of infrastructure possible, which of the available Ethereum algorithms is more efficient for a Private network? In this study, we implement two instances of the Ethereum Blockchain with different consensus algorithms in order to explore which one will be the most efficient and cost-effective in an enterprise environment.*

Key Terms – *Bitcoin, Blockchain, Consensus Algorithms, Smart Contracts.*

BLOCKCHAIN TECHNOLOGIES

Blockchain started in 2008 when the pseudonym Nakamoto published a paper describing the theory behind the digital currency Bitcoin (Nakamoto, 2008) [1]. Transactions between individuals are secured by cryptography, broadcasted peer-to-peer, verified by nodes in a network and the history of transactions are distributed to all nodes in the network [2]. At their most basic level, they enable a community of users to record transactions in a ledger that is public to that community, such that no transaction can be changed once published [2]. This technology enables it's users to process transactions on the same platform and the same ledger with the potential to optimize the industries that exchange physical goods.

As seen in figure 1, enterprises today that share information or goods have to store their own ledger information or inventory, versus with a blockchain environment where everyone connects to the blockchain and can interact with the same information without having inherent trust with each other. Technically Blockchain is a sequence of blocks, where each block contains a list of transactions like conventional public ledger [3].

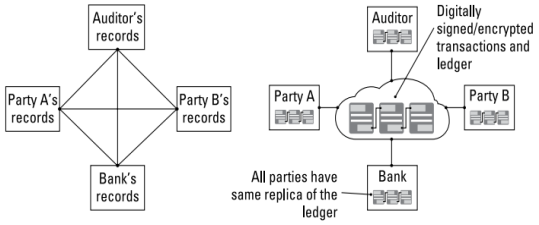

Figure 1
Current Networks vs Blockchain Networks [4]

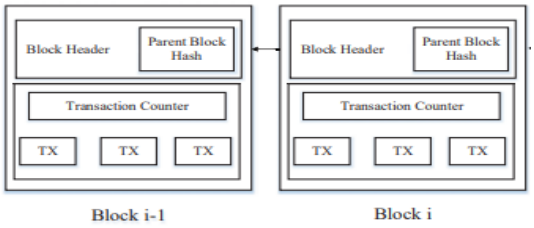

Figure 2
Blockchain Structure [3]

Inside each block you can also find a hashed number representing the previous block of the chain, a block header and a block body. More recently we have seen the inclusion of code transactions inside the blockchain called smart contracts. A smart contract is an agreement or set of rules that govern a business transaction; it's stored on the blockchain and is executed automatically as part of a transaction [4]. This has enabled a whole new breed of applications called Decentralized Applications (Dapps).

BLOCKCHAIN USE CASES

With the implementation of smart contracts, you can leverage the benefits of Blockchain technologies for integrated solutions in Finance, Supply Chain,

Government and other industries/entities where transactions are required to be immutable, auditable, accessible and distributed inside a network of nodes. Some of the use cases that benefit from blockchain are:

- Trade finance where you can streamline the process of obtaining approvals from multiple legal entities like customs, port authorities, transportation and logistics [4].
- Cross-border transactions where you can transfer funds directly to the other person/persons without having to pass with the current settlements in the banking industry [4]. Insurance can automate the claims processing in order to have automatic payouts when the customer provides with the required information of the incident [4].
- Governments can have great benefits of having a single true identity system that identifies the citizens in a decentralized platform, healthcare industry can have a secure and efficient record management system where all of the patients information lives in a single Blockchain regardless of the hospital or doctors involved [4].
- Internet of Things and how computers continuously communicate with one another that will get complemented with Blockchain by providing the immutable ledger where to store the information from the IoT devices [4].

For example the IBM Watson IoT platform built-in capability also allows users to add selected IoT data to private blockchain ledgers that can be included in shared transactions. The platform translates the data from connected devices into the format that blockchain contract APIs need [5].

ETHEREUM BLOCKCHAIN

Ethereum is a blockchain platform focused on providing smart contracts. Smart contracts are programs that exist on the blockchain that can be accessed by Ethereum users. Ethereum's transaction programming language is Turing complete. Where the mining nodes receive funds through mining and transaction fees [2]. This platform has become the de-facto smart contract blockchain due to its wide acceptance as a public platform for decentralized apps (Dapps). Ethereum being open sourced has received multiple implementations in different languages. One of the most popular implementations is the Golang Ethereum client called Geth [6]. This client can manage wallets, miners and even a private network with multiple nodes. Currently, Ethereum shares the same mining algorithm as Bitcoin called Proof of Work, but since March 2017 the Geth project received a proposal to implement the algorithm Proof of Authority called Clique. With this proposal, Geth becomes a better alternative to be utilized with private networks because by theory you don't need miner nodes, you will have approval nodes that reach consensus with less effort.

CONSENSUS ALGORITHMS - PROOF OF WORK

The consensus algorithm Proof of Work is a solution implemented initially by Bitcoin and also integrated into Ethereum in order to solve the concern of trust between the nodes participating in the public network. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits [7]. This hashed value gets added to the chain and the complexity of the number of zeroes gets incremented. Once you start adding blocks if you wanted to change anything in the chain, you would have to redo the work of all of the blocks after that block. This way the process resolves the trust issue by investing extensive CPU/GPU power in the chain with the theory that if a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains [7].

CONSENSUS ALGORITHMS - PROOF OF AUTHORITY

Upon understanding the concepts of Proof of Work and the intensive computational power that it

is required, there must be another way to provide block consensus designed for private Ethereum networks. That is precisely what was recommended within the Ethereum's project Ethereum Improvement Proposal repository on March 6th, 2017 where an alternate consensus algorithm was proposed for both the test network Rinkeby and an alternative in the client for private networks [8].

In a nutshell Proof of Authority is a protocol/algorithm where instead of miners racing to find a solution to a difficult problem, authorized signers can at any time at their own discretion create new blocks [8].This is consensus algorithm is viable in a private network because you have to pre-approve (whitelist) the initial specific nodes that will be trusted to decide which blocks will be added into the blockchain. Hence participants should be able to rely on that fact and so that one confirmation should be enough for finality [9]. Even though you have the previous assumptions, the implementation of PoA has to take into consideration the possibility of malicious approval nodes and the amount of damage they can do in the network. In the Ethereum implementation of PoA there are multiple safeguards embedded in the solution mentioned in [8] but in particular, the main safeguard is that any approving node may only create a block out of half of the number of signin nodes. This ensures that the malicious entity must take control of about 51% of the nodes in the private network.

PROOF OF WORK VERSUS PROOF OF AUTHORITY - COMPARISON

The basis of PoA is to optimize hardware utilization for a private network, but how much will be this improvement in hardware utilization when compared to a PoW with low complexity implementation? This is the initial question to answer when evaluating the configurations and hardware requirements of a private Ethereum blockchain implementation for the enterprise.

As part of this study we want to compare the two algorithms in separate private implementations eliminating as many environment variables as possible by utilizing the following implementation/infrastructure:

- Two AWS m4.large server with 2 vCPUs, 8GB of RAM and 100GB of storage for the Proof of Authority implementation.
- Two Microsoft Azure nodes with 1 vCPU each, 3.5GB of RAM and 50GB.
- AWS CloudWatch for CPU consumption measurement.
- Microsoft Azure CPU monitor.
- Go Ethereum implementation with two synchronized nodes for each server/implementation.
- Eth Netstats implemented on each server for blockchain performance measurement.
- One Reactjs application that interacted with a smart contract implemented in both networks for user experience comparison using the Meta Mask wallet.

Since the algorithms utilize different parameters, we began the initial tests by executing both algorithms as fast as they could run. For Proof of Work we configured the mining complexity to 1 and for Proof of Authority, we configured the nodes to sign 1 block per second.

The initial comparison after starting up both networks was a CPU measurement. Even though we expect that PoA will be more efficient in CPU consumption since it doesn't have to execute the mining process, we didn't expect to have such a big difference between each server utilization.

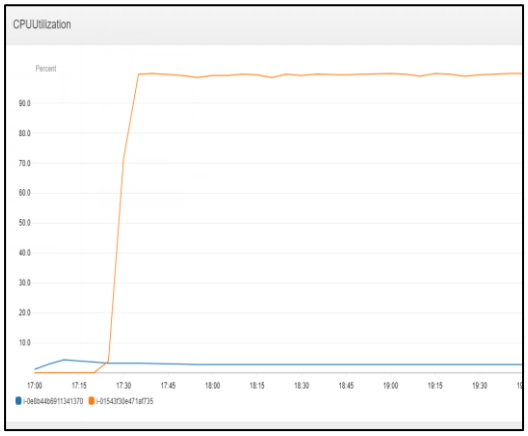

Figure 3
CPU Consumption: AWS Blue (PoA) versus Orange (PoW)

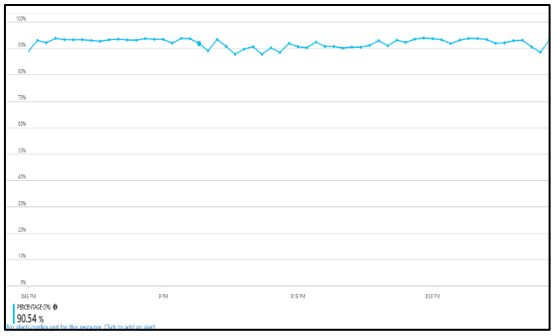

Figure 4
CPU Consumption: Azure Ethereum Implementation (PoW)

Secondly, we need to compare the blockchain performance of each implementation. Within the plethora of information provided by eth-netstats we can compare key fields like the average block time between networks as seen below:

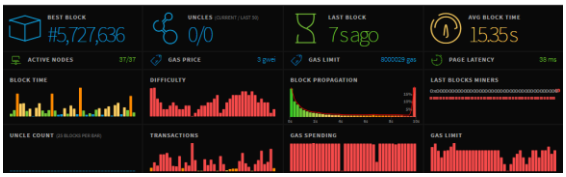

Figure 5
Public Ethereum Net Stats (15s Avg. Block Time)

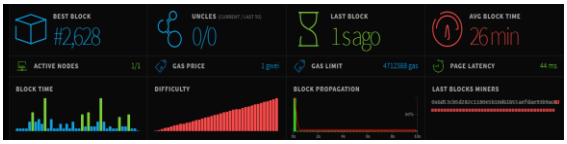

Figure 6
Private PoW Ethereum Net Stats (26m Avg. Block Time)

Figure 7
Private PoA Ethereum Net Stats (1s Avg. Block Time)

We can see how PoA is consistent with that is expected from this algorithm of producing blocks at the specified 1 block per second versus the PoW network which is suffering from lack of processing power in order to mine fast enough to be comparable to the 15s block time of the Ethereum public network.

The final comparison test was the User Experience comparison where we implemented a simple solidity contract in both instances, a Reactjs website that communicated with each instance with the chrome addon Meta Mask wallet that is used to store the Ethereum accounts and pay any transaction fees. The main task of this application is to store and change a string called state. The test consisted in executing 20 consecutive state changes and measuring the amount of time, with the in-browser console, it took from submitting to changing the state in the network.

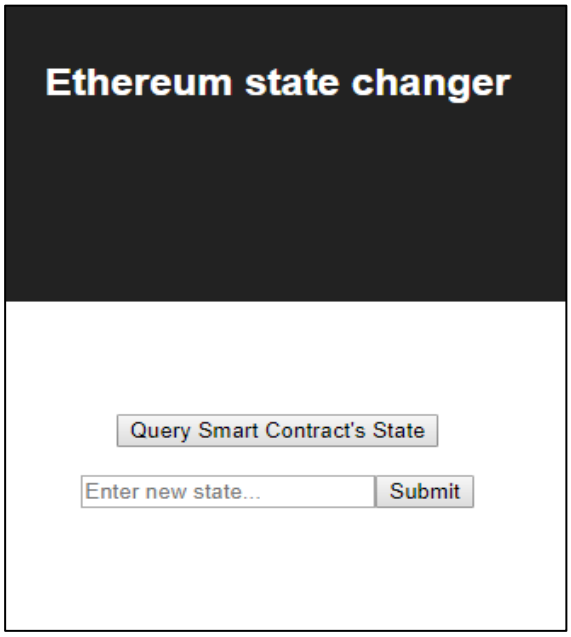

Figure 8
Reactjs Application that Interacts with the Smart Contract

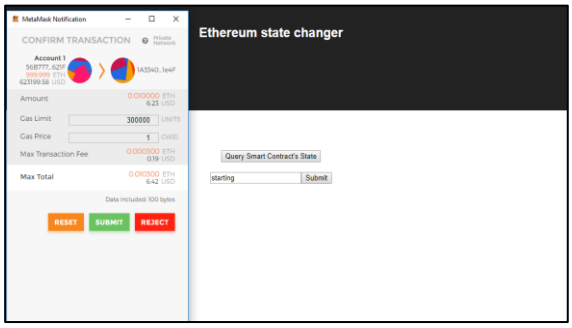

Figure 9
Approving the Contract Utilization with Meta Mask

Upon having problems in submitting and interacting with the solidity contract for PoW, we implemented the Azure consortium and executed 20 smart contract interactions and measured the time it takes for the contract to be modified in the blockchain in the figure below.

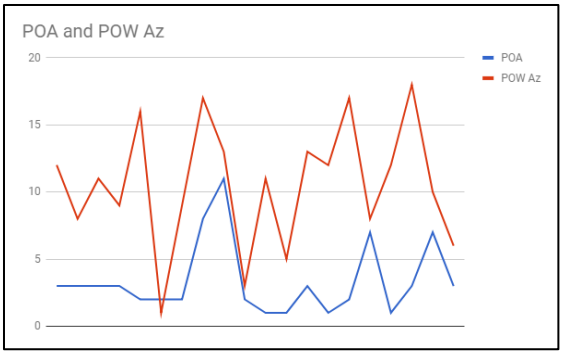

Figure 10
Transaction Response Time between PoA and PoW

As seen in the figure above, Proof of Authority was consistently faster in the time it took to change the state of the smart contract in the blockchain.

CONCLUSION

After completing the study with the different tests executed we can confirm that not only the Proof of Authority consensus algorithm is faster in producing the blocks and processing blockchain requests, it is also remarkably efficient in the CPU consumption, enabling the enterprise implementations to create ethereum networks at a reduced cost.

Even though we were able to identify a preferred consensus algorithm for a private network, we are still left with a lot of scalability questions before this technology/algorithm can be taken into consideration for an enterprise level solution. For example,

- How many nodes is it recommended for a PoA production environment?
- Which hardware is recommended for a PoA network?
- How much of an impact the latency of having nodes in different datacenters will impact the network's response time?
- How can signin nodes be integrated in the blockchain automatically?
- When will storage and the size of the blockchain will become an issue? Since each block is stored in the system even if it doesn't have any transactions in it.
- How fast are we going to sign blocks in the blockchain?

One important point to consider with PoA is that we can't add as much nodes as we want and expect it to work more resiliently, because If N sealers are defined in the genesis file, clique will only work if int(N/2+1) nodes are online. So with PoA for 4 and for 5 nodes you will need 3 mining/signin nodes for the network to work [8]. On the other hand PoA is one of the more recent consensus algorithms that we have proved that it is a great contender to be used in an enterprise level implementation and it will even save operational costs for the sole reason that we can use less hardware for the same results.

FUTURE WORK

For future work, we want to expand both the scope of the user experience tests by creating a more realistic and complex smart contract and automating the user interaction to measure load capacity. We want to continue answering the scalability questions identified as a result from this study and we also want to compare this solution with other technologies specifically designed for private networks, because even though this is more efficient that PoW, we are still using Ethereum that was designed as a public network Blockchain, where other technologies introduce by design more security, privacy and flexibility that are essential in a private enterprise network.

Some of the technologies that we want to expand the comparison directly are Blockchain technologies that support solidity contracts designed for private networks: JP Morgan's Quorum and Hyperledger's Sawtooth. We also want to see how this implementation measures out with other Blockchain technologies for the enterprise like Hyperledger's Fabric and R3 Corda.

REFERENCES

[1] P. Corten. (2018, March 5th). *Blockchain Technology for Governmental Services: Dilemmas in the Application of Design Principles* [Online]. Available: https://repository.tudelft.nl/islandora/ object/uuid:87709465-b9a1-48da-9ba5-eba98bc263d7/datastream/OBJ1/download.

[2] D. Yaga, et al. (2018, January). *Blockchain Technology Overview* [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/ nistir/8202/draft/documents/nistir8202-draft.pdf.

[3] Z. Zheng, et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *IEEE 6th International Congress on Big Data*, June 2017.

[4] M. Gupta, *Blockchain for Dummies*®, IBM Limited Edition. John Wiley & Sons, Inc, 2017.

[5] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?" in *IEEE IT Professional*, vol. 19, no. 4, pp. 68-72, 2017.

[6] Ethereum Community. (n. d.). *Ethereum Homestead Documentation* [Online]. Available: https://media.readthedocs.org/pdf/ethereum-homestead/latest/ethereum-homestead.pdf.

[7] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System* [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[8] P. Szilágyi. (2017, March 6th). *Clique PoA protocol & Rinkeby PoA testnet* [Online]. Available: https://github.com/ethereum/EIPs/ issues/225.

[9] D. Baars. (2016, June 23rd). *Towards Self-Sovereign Identity using Blockchain Technology* [Online]. Available: http://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf.