VIVA-Tech International Journal for Research and Innovation *Volume 1, Issue 4 (2021)*
ISSN(Online): 2581-7280
VIVA Institute of Technology
9thNational Conference onRole of Engineers in Nation Building – 2021 (NCRENB-2021)

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

BLOCKCHAIN SHARDING

Sreeraj Menon[1], Prof.ChandaniPatel[2]
[1](Department of MCA, VIVA SCHOOL OF MCA/University of Mumbai, India)
[2](Department of MCA, VIVA SCHOOL OF MCA/University of Mumbai, India)

Abstract-*Bitcoin has been a hot topic in the technology industry since its boom in 2017. The underlying technology of bitcoin is the blockchain that has impressed many of the onlookers due to its transparency and usability in this globalized world. In cryptocurrencies, a ledger is operated which contains all the data regarding the transactions and contracts that are to be executed. These ledgers are maintained on multiple nodes around the world. Every node has to maintain a full copy of the ledger which currently is 15 GB for bitcoin. As more and more transactions are carried on the blockchain, this approach becomes slow. Scaling is the only solution to counter this problem, that's where the sharding technology comes into play. In sharding, rather than each node maintaining the full ledger, the ledger is divided or sharded into multiple fragments. So, in short, each node consists of a small part of the ledger rather than the whole ledger which is easy to maintain and in turn helps in scaling the blockchain. So rather than a full blockchain, we have shard chains that consist of multiple node or validator networks which are then assigned multiple tasks like verifying transactions or operations.*

Keywords- *Blockchain, Consensus, Hashing, Ledger, Sharding.*

I. INTRODUCTION

Most of the financial system in the 21st century is still under a centralized entity or a group of exclusive entities. However, this kills the basic principle of financial freedom which can be easily attained in a decentralized environment. This is where the idea of blockchain comes into the picture. Although most people got to know about blockchain through the boom or popularity of bitcoin in early 2008. However, blockchain is not limited to bitcoin or any other cryptocurrency, there are a plethora of other opportunities that can be unlocked, like for example, we can implement it for voting systems that can fulfil the needs of a transparent democracy. As it doesn't come under the power of a single entity there is no chance of manipulating the data or deleting it.
Blockchain technology provides great opportunities to promote various sectors through its unique combination of features, for e.g., decentralization, consistency, and transparency. We see promising opportunities in the application of this scientific and academic technology.

Blockchain has revealed its great capability in disrupting how digital dealings are passed out in a more protected and transparent manner. But the question still stands - does it have the capability to assist other practical applications? Such misperception is because of the interruption caused by its scalability problems. Scalability issues rise due to inadequate block size and present consensus method where each node in the system consecutively authenticate the contract before it being issued in the blockchain. This problem deepens with a rise in the number of dealings requiring additional nodes to support the system but at the same stretch increasing the number of steps for the contract to travel and spread complete consensus with each node. We can also get a comparative relationship among decrease in scalability of the blockchain and increase in the system size. This flaw is the key setback that is discontinuing the mass approval of blockchain for real-life applications.

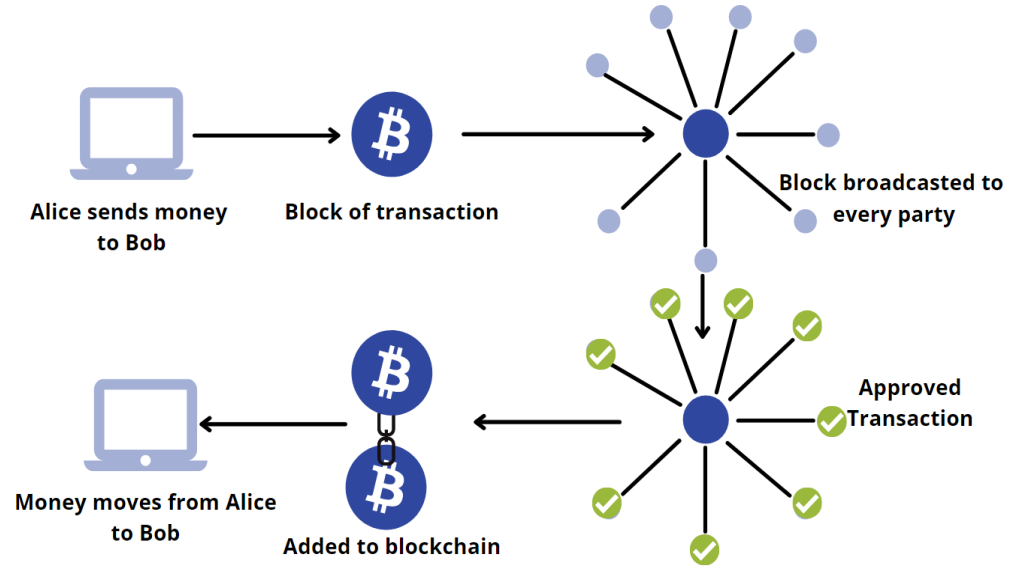

Figure.1 Basic representation of a transaction getting executed on blockchain

Consensus is one of the utmost significant problems in blockchain, as in any dispersed systems where numerous nodes must reach a contract, even in the occurrence of faults. Existing consensus algorithms stay only valid to limited systems because of difficulty, e.g., the Practical Byzantine Fault Tolerance protocol (PBFT) [1] with fewer than 20 active nodes. Scalability is a problem that has to stay addressed before accepting blockchain in extensive applications. Lately, many resolutions have been projected to attain the scale-out amount by permitting participating nodes only to obtain a portion of the entire business set, for instance, an Off-chain resolution, Directed Acyclic Graph (DAG) [2] and blockchain sharding [3]. However, the offchain resolution is more focus to forks and the dealings in the DAG layout are not systematized in a chain construction. Among all the planned methods, sharding systems look like the most effective as they can overcome operational difficulties and scalability problems equally. A sharding arrangement splits the giving out of transactions amongst minor clusters of nodes, called shards. As an outcome, shards can work in parallel to maximize the act and progress the throughput while demanding significantly less communication, computation, and storage overhead, letting the system to work in large schemes.

II. DIFFERENT CONSENSUS ALGORITHMS

Before getting into details about sharding, let us figure out the different consensus protocols used in the blockchain ecosystem to agree upon a certain transaction or contract. These are the most common consensus mechanisms used currently in the blockchain ecosystem-

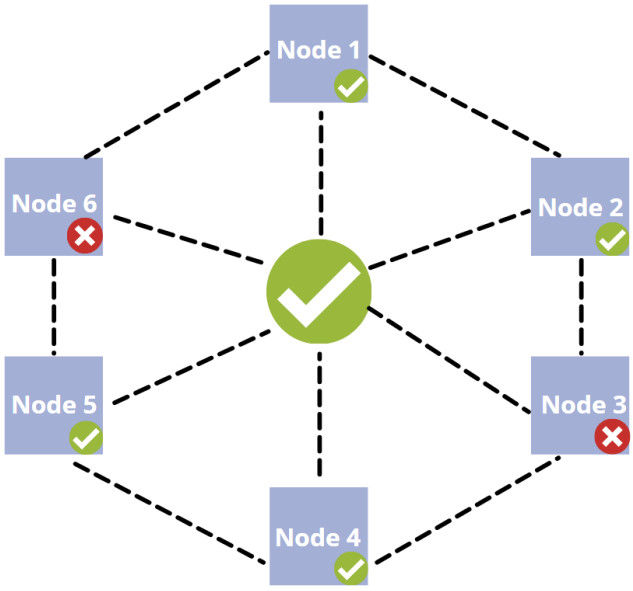

Figure.2 Basic consensus mechanism on the blockchain

2.1Proof of Work (POW):

POW is the primary and most familiar consensus mechanism and developed by Bitcoin's founder, Satoshi Nakamoto. In POW, a miner who discovers the hash first will be permitted to enhance a new block of the contract to the blockchain. The method of mining is enormously computation-intensive, so taking a high hashrate is the key for miners to analyze the hash, thus receiving the rewards. Besides Bitcoin, Ethereum is also using POW as a part of their algorithm. However, what makes Ethereum different is their proof of stake (POS)-based finality system capable of overlaying a prevailing POW blockchain, resulting in a hybrid POW/POS system called Casper Friendly Finality Gadget (FFG).

2.2Proof ofStake (POS):

Proof of Stake is a agreement algorithm in which the stake-holders who need to contribute in the validation process, are obligatory to lock a certain quantity of coins into the system as their stake. A stake-holder of a agreed blockchain is an individual holding roughly native coins of that blockchain, and stake positions the native coin holding of a stake-holder. For instance, on the ethereum network, the stake would be the quantity of ether held by a node.

2.3Delegated Proof of Stake (DPOS):

Delegated proof of stake is a fresher and progressive consensus mechanism grounded on the old-style proof of stake. The system was established by Daniel Larimer in demand to speed up dealings and creation of block while preserving the decentralized incentive assembly in the blockchain. Blockchains counting EOS, Steemit have accepted the DPoS system. The key aim behind generating DPoS is to shape a system that is fast, scalable and pursues consensus more professionally. It uses a voting scheme to select the observer (validator) to grasp consensus in the blockchain.

2.4Practical Byzantine Fault Tolerance

Practical Byzantine Fault Tolerance is a consensus algorithm announced in the late 90s by Barbara Liskov and Miguel Castro. pBFT was planned to labor competently in asynchronous (no higher bound on when the response to the request will be acknowledged) systems. It is enhanced for short overhead time. Its goal was to

solve many difficulties associated with already existing Byzantine Fault Tolerance solutions. Application areas contain distributed computing and blockchain.

2.5Directed Acyclic Graph

DAG-based protocols mostly vary in how dealings are added to a network. Contrasting blockchain technology, specific DAG transactions are related to one another directly rather than combined together in blocks and handled. Since this assembly can reference various "blocks" at one time, the transactions per second, or TPS, rate is very much higher than that of a typical blockchain. Bitcoin's TPS varies anywhere between 4 to 7, Ethereum sits at 30, and central legacy services like Visa support throughput rates of around 1,000 TPS. Nowadays, some DAG-based protocols can handle a TPS frequency into the numerous thousands.

III. SHARDING OVERVIEW

In this paper, we take a upright method to spread sharding to permissioned blockchain structures. Present works on sharded blockchains mark permission less systems and stress on security. Here, our focus is on performance. In specific, our goal is to project a blockchain system that can deliver a big network size alike to that of major cryptocurrencies like Bitcoin [4] and Ethereum [5]. At the similar time, it accomplishes high deal throughput that can handle the usual workloads of centralized systems such as Visa, which is around 2, 000−4, 000 dealings per second [6]. Finally, the system chains any blockchain application from domains such as finance [7], supply chain management [8] and healthcare, not being inadequate to cryptocurrencies. Sharding protocols have been widely considered in distributed database systems. A sharding protocol must ensure both atomicity and isolation of deal execution. State-of-the-art protocols goal to recover performance for distributed dealings in geo-replicated settings. However, they cannot be directly extended to blockchain systems, due to an important difference in the failure models that databases and blockchains consider. Traditional databases assume the crash-failure model, in which a faulty node simply halts sending and responding to requests. On the other hand, blockchain systems operate in an additional hostile environment, therefore they adopt a stronger failure model, namely Byzantine failure, to account for malicious attackers. Figure 1 highlights the transformations between spread databases and sharded blockchains. The distinction in failure models leads to three challenges when smearing database sharding techniques to blockchains. First, high performance consensus protocols used in distributed databases, cannot be applied to blockchains. Instead, blockchains rely on Byzantine Fault Tolerance (BFT) consensus protocols[9] which have been shown to be a scalability bottleneck. Therefore, the primary challenge is to scale BFT consensus protocols. Additionally, in a distributed database any node can fit to any shard, but a blockchain must allocate nodes to shards in a safe manner to guarantee that no shard can be conceded by the attacker. The second task, thus, is to achieve protected and efficient shard creation. Third, the distributed database depends on on highly accessible transaction coordinators to safeguard atomicity and separation, but coordinators in the blockchain may be malicious. Subsequently, the third challenge is to allow secure distributed transactions even if the coordinator is malicious.

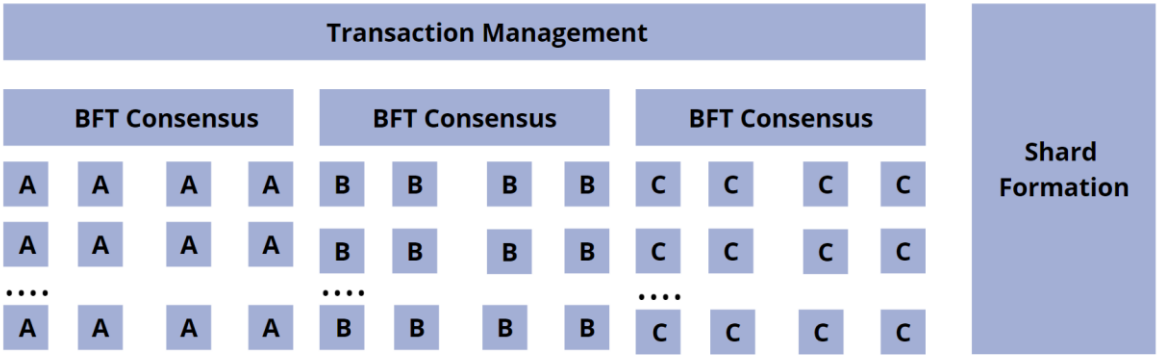

Figure.3 Sharded Blockchains

IV. CROSS SHARDING TRANSACTION

To scale blockchain, dealings need to be dispersed among several groups (or shards), and individually shard processes a subsection of transactions in parallel. Classically, a transaction may consume multiple inputs and outputs. But, due to sharding technology, the inputs and outputs of a transaction may be in different shards, and these dealings are called cross-shard (or inter-shard) dealings. Due to random distribution of the transactions in sharding protocols, a cross-shard deal can be measured as a global transaction, which must be performed by multiple different shards. To attain a global consistency amongst different shards, we want to cautiously handle the cross-shard transactions. Taking the Unspent Transaction-Output (UTXO) model [10] as an example, it is possible that most transactions (e.g., more than 90% in general [11]) are separated by the old-style model, in which UTXOs improperly allocates processing shards. For the Account/Balance transaction model, the cross-shard transactions also can grasp up to 90% once the number of shards is more than 64 [12]. To allow the transfer of value between different shards thus achieving minimal interaction, support for cross-shard transactions is essential for any sharded-ledger structure [13].For the cross-shard dealings, the protocol needs to promise the atomic possessions [14]. Lastly, a reconfiguration process is wanted at the end of an epoch [15].

V. CONCLUSION

This paper presents a categorization of information related to sharding on blockchain. We recognized important mechanisms and tasks in sharding. The freely verifiable unpredictability is critical for employing participating nodes consistently into shards. Inside each shard, a consensus protocol is required to reach an agreement on the blocks. BFT-based protocols are controlling in current solutions. We analysed numerous renowned blockchain sharding procedures and then discussed several potential research directions. There are many drawbacks in the blockchain ecosystem with scaling being one of the few, it can be achieved easily by applying a concept like sharding. Sharding not only makes transactions fast, but also makes the blockchain more secure by multiple the ledger into different shards. This can also prevent the take over or control over done by a single or group of entities, there by making it more decentralized. Decentralized in the sense, by giving more power to the masses, through governance protocols and mechanisms. There are much more that needs to be done before jumping on to sharding, but nonetheless sharding can improve the ecosystem of a whole blockchain by making it more fresh and quicker than before.

ACKNOWLEDGMENTS

This research was supported by Prof. Chandani Patel. We thank our colleagues from Viva School of MCA who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.

REFERENCES

[1] Castro, M., Liskov, B., et al. *Practical byzantine fault tolerance*. In OSDI (1999), vol. 99, pp. 173–186.
[2] Popov, S. *The tangle*. cit. on (2016), 131.
[3] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., and Saxena, P. *A secure sharding protocol for open blockchains. In proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (2016), ACM, pp. 17–30.
[4] Satoshi Nakamoto. 2008. *Bitcoin: A peer-to-peer electronic cash system.*
[5] Vitalik Buterin. 2014. *Ethereum: A next-generation smart contract and decentralized application platform.* https://github.com/ethereum/wiki/wiki/White-Paper (2014).
[6] Bitcoin Wiki. 2018. Scalability. en.bitcoin.it/wiki/scalability
[7] Ripple. https://ripple.com
[8] Fr8 Network. 2018. *Blockchain enabled logistic*. https://fr8.network.
[9] Miguel Correia, *Essentials of Blockchain Technology* (CRC Press, 2019).
[10] Andreas M. Antonopoulos, *Mastering Bitcoin* (O'Reilly Media, Inc.,2014)
[11] Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., and Ford, B. Omniledger: *A secure, scale-out, decentralized ledger via sharding. In 2018 IEEE Symposium on Security and Privacy* (SP) (2018), IEEE, pp. 583–598.
[12] Wang, J., and Wang, H. *Monoxide: Scale out blockchains with asynchronous consensus zones*. In 16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 19) (2019), pp. 95–112.
[13] Alex Skidanov, *Nightshade:Near Protocol Sharding Design* (2019).
[14] Bob Gregory, *Technology of Atomic Swaps* (2015).
[15] Medjitena Nadir, *A practical guide to blockchain business* (2018).