**Literature Survey on Consensus Algorithm**

|  |  |  |
| --- | --- | --- |
|  | Permissionless (Public) Blockchain | Permissioned (Private) Blockchain |
| Acess | Open read/write | Permissioned read and/ or write |
| Speed | Slower | Faster |
| Consensus Algorithm | Proof of Work  Proof of Stake | Pre-approved participants |
| Identity | Pseudonymous | Known identities |

**Fig.1.** Classification of Blockchain

Fig.1. enlists the various distinguishing criteria for classifying the types of blockchain [1].The consensus algorithm evaluates the criteria’s and circumstances that are to be reached in order to validate the blocks that are to be included in the blockchain. The consensus algorithm is an outcome of the Byzantine Generals’ Problem which states that any two devices on the decentralised unreliable network cannot completely and indisputably ascertain that they are representing the same data. The Byzantine Fault Tolerance is an attribute which denotes the tough set of defective nodes that are associated with the Byzantine Generals’ Problem. It can tolerate up to 33% defective nodes that is 3f+1 where f is the total number of faulty replicas present in the system [2]. Typically, there are four proofs used to implement the consensus algorithm. The Proof of work (PoW) is a consensus algorithm used in public blockchain like bitcoin and has proven itself to be successful against Sybil attacks [3]. It involves the concept of mining for adding new blocks by solving a hash puzzle. PoW has its own limitations [4]. It makes use of exhaustive computations and consumes lot of electricity for mining. A common security approach is to accept the changes made in the last block only after the transactions are confirmed in the previous six blocks. This takes almost an hour and thus restricts the usability and applicability of the present day PoW Blockchain technologies. In Proof of Stake (PoS) consensus algorithm the block validator constructs a hash from the collection of data indicating the currency owned by the validator and the duration of ownership. The participant needs to put certain crypto coins at stake to verify the transactions. The block validator is then chosen pseudo-randomly based on the participant’s wealth and coins at stake. The hash function is rerun with the latest timestamp as input in case the hash function does not start with a particular number of zeroes [5]. In Delegated Proof of Stake (DPoS) introduced by Daniel Larimer stakeholders elect the members (witnesses) responsible for block creation. The witnesses generate a block only when it is their turn to do so. If the witness fails in producing the block they are removed from future elections. The blocks are produced after every three seconds and the producers are re-arranged after every 21 blocks. Every voter is given an importance according to their crypto coins at stake [6]. Typically the top 20 witnesses are rewarded for verifying the transactions. DPos is significantly faster and scalable than PoS due to lesser number of participants responsible for block creation and validation. Proof-of-Authority (PoA) is a replacement for Proof-of-Work, which can be used for private chain setups, uses a set of “authorities” - nodes that are explicitly allowed to create new blocks and secure the blockchain. The chain has to be signed off by the majority of authorities, in which case it becomes a part of the permanent record. This makes it easier to maintain a private chain and keep the block issuers accountable. PoA is secure, scalable and interoperable.

For e.g. Oracle's Network is open public permission network based on ethereum protocol with proof of authority consensus reached by independent pre-selected validators. Validators are service authorities who secure the network and seal the blocks. They are the known individuals with active notary public license that means that all their information is in the public domain and any third party can check their identity. With no mining or stake required Oracle's network makes smart contract platform cheaper and faster. It makes open networks more affordable for small and medium businesses.

The blockchain node network administrators are responsible for following governance-spawned functions [7]:

* Assigning and retaining roles/permissions that are used to authorize node activity to trusted and capable participants
* Securing public and private keys for authentication and authorization purposes
* Encrypting data via instituted cryptography practices
* Storing rules that represent smart contracts, and for the invoking of these
* Formulating and instituting consensus validation algorithm(s)
* Maintaining a node’s processing history, and its degree of success
* Recording of service level agreements (e.g., performance, uptime), as approved by the node network administrators
* Managing and monitoring of network performance by:
  + Balancing the load among the nodes
  + Detecting rogue threats and malicious activity
  + Monitoring the machine state of the network (e.g., nodes are operational and in-synch)
  + Evaluating a node’s processing performance against any service level agreement measurements

PoA algorithms favour availability over consistency [8]. Proof-of-Authority (PoA) is a new family of BFT (Byzantine fault tolerant) algorithms which has recently drawn attention due to the offered performance and toleration to faults. PoA requires less message exchanges hence provides better performance. Table 1 depicts the differences between the various consensus algorithms discussed so far [9].

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | PoW | PoS | DPoS | PoA |
| Principle | The solution is complex to deduce but convenient to validate. | Higher the stake of a validating node in the network, the more chances and legitimacy it has to validate transactions. | Panel of delegates elected by users of the network monitor the blockchain and propose changes to the protocol which must be approved by the users. | Blocks are validated if signed by a specified quorum of signers. |
| Node Identity Management | Open | Open | Open | Permissioned |
| Energy Saving | No | Partial | Partial | Yes |
| Tolerated Power of Adversary | <25% computing power | <51% stake | <51% validators | <33.33% validators |
| Throughput(TPS) | <100 | <1000 | <1000 | <2000 |
| Scalability | Strong | Strong | Strong | Weak |

**Table 1.** Comparison of various Consensus Algorithms

Two of the main PoA algorithms are AuRa and Clique. Proof of Authority (PoA) is a family of consensus algorithms for permissioned blockchain. PoA algorithms rely on a set of N trusted nodes called the authorities. Each authority is identified by a unique id and a majority of them is assumed honest, namely at least N/2 + 1.

AuRa is the name for Parity's Proof-of-Authority (PoA) consensus engine, the name originally comes from Authority Round (used to be AuRo). It's used in the Kovan network. In AuRa, each block proposal requires two message rounds: in the first round the leader sends the proposed block to all the other authorities, in the second round each authority sends the received block to all the other authorities. A block is committed after a majority of authorities have proposed their blocks, hence the latency in terms of message rounds in AuRa is 2( N/ 2 + 1), where N is the number of authorities. In Clique, a block proposal consists of a single round, where the leader sends the new block to all the other authorities. The block is committed straight away; hence the latency in terms of message rounds in Clique is 1. Such a huge difference between AuRa and Clique is due to their different strategies to cope with malicious authorities aiming at creating forks: AuRa waits that enough other blocks have been proposed before committing; Clique commits immediately and copes with possible forks after they occur. Clique seems to outperform PBFT too, which takes three message rounds to commit a block. So the number of authorities has a linear relationship with the latency (in terms of message rounds) in case of AuRa. If the number of authorities increases the latency (in terms of message rounds) will increase. On the other hand latency (in terms of message rounds) remains unaffected by the number of authorities. The number of validators(authorities) shall be restricted if a blockchain network is using AuRa consensus algorithm.

AuRa makes use of three parameters:

1. N: the number of nodes
2. f: the number of faulty nodes
3. t: the step duration in seconds

Time is divided into discrete steps of duration t, determined by UNIX time/t. The index s of each step is deterministically computed by each authority as s = t/step duration, where step duration is a constant determining the duration of a step. The leader of a step s is the authority identified by the id l = s mod N. Authorities maintain two queues locally, one for transactions Qtxn and one for pending blocks Qb. Each issued transaction is collected by authorities in Qtxn. For each step, the leader l includes the transactions in Qtxn in a block b, and broadcasts it to the other authorities. Then each authority sends the received block to the others (round block acceptance). If it turns out that all the authorities received the same block b, they accept b by enqueuing it in Qb. Any received block sent by an authority not expected to be the current leader is rejected. The leader is always expected to send a block, if no transaction is available then an empty block has to be sent. If authorities do not agree on the proposed block during the block acceptance, a voting is triggered to decide whether the current leader is malicious and then kick it out. An authority can vote the current leader malicious because (i) it has not proposed any block, (ii) it has proposed more blocks than expected, or (iii) it has proposed different blocks to different authorities. The voting mechanism is realised through a smart contract, and a majority of votes is required to actually remove the current leader l from the set of legitimate authorities. When this happens, all the blocks in Qb proposed by l are discarded. Note that leader misbehaviours can be caused by benign faults (e.g., network asynchrony, software crash) or Byzantine faults (e.g., the leader has been subverted and behaves maliciously on purpose). A block b remains in Qb until a majority of authorities propose their blocks, then b is committed to the blockchain. With a majority of honest authorities, this mechanism should prevent any minority of (even consecutive steps) Byzantine leaders to commit a block they have proposed. Indeed any suspicious behaviour (e.g., a leader proposes different blocks to different authorities) triggers a voting where the honest majority can kick the current leader out, and the blocks they have proposed can be discarded before being committed.

Clique [10] is another PoA algorithm employed in Geth [11]. The algorithm executes in time divisions which are recognised by a prefixed order of committed blocks. When a new period starts, a special transition block is broadcasted. It specifies the set of authorities (i.e., their ids) and can be used as snapshot of the current blockchain by new authorities needing to synchronise. While AuRa is based on UNIX time, Clique computes the current step and related leader using a formula that combines the block number and the number of authorities. Most of all, in addition to the current leader, other authorities are allowed to propose blocks in each step. To avoid that a single Byzantine authority could wreak havoc the network by imposing a sheer number of blocks, each authority is only allowed to propose a block every N/2+ 1 blocks. Thus, at any point in time there are at most N − (N/2 + 1) authorities allowed to propose a block. Similarly to before, if authorities act maliciously (e.g., by proposing a block when they are not allowed) they can be voted out. Specifically, a vote against an authority can be casted at each step and if a majority is reached the authority is removed from the list of legitimate authorities. As more authorities can propose a block during each step, forks can occur. However, fork likelihood is limited by the fact that each non-leader authority proposing a block delays its block by a random time; hence the leader block is likely to be the first received by all the authorities. If forks happen, the GHOST protocol [12] is used, which is based on a block scoring approach: leaders’ blocks have higher scores, thus ensuring that forks will be eventually solved.

## Though PoA is best suited for private blockchains it still faces a lot of challenges. First, it strongly lack decentralization. Second, PoA suffers from the problem of censorship. Third, chances are that signer key/machine may get compromised and lead to the addition of malicious user to list of valid signers.

## Consensus algorithm is the core technology of blockchain, yet the present day research of the consensus mechanism is still in its infant stage. The consensus algorithm specially designed for different scenarios is still very seldom. “How to enhance the performance of the blockchain in a particular scenario?” is still a question requiring further research to be answered.

**References:**

1. Chris Skinner’s Blog: https://thefinanser.com/
2. L.M. Bach, B. Mihaljevic and M. Zagar, “Comparative analysis of Blockchain Consensus Algorithms”, MIPRO 2018, May 21-25, Opatija Croatia, 1545-1551
3. John R. Douceur, “The Sybil Attack”, International Workshop on Peer-to-Peer Systems, IPTPS 2002: Peer-to-Peer Systems pp 251-260
4. Bozhi Wang, Shiping Chen, Lina Yao , Bin Liu, Xiwei Xu and Liming Zhu, “A Simulation Approach for Studying Behavior and Quality of Blockchain Networks”, Springer International Publishing AG, part of Springer Nature 2018 S. Chen et al. (Eds.): ICBC 2018, LNCS 10974, pp. 18–31, 2018. https://doi.org/10.1007/978-3-319-94478-4\_2
5. https://spectrum.ieee.org/computing/networks/how-blockchains-work
6. https://hackernoon.com/the-difference-between-traditional-and-delegated-proof-of-stake-36a3e3f25f7d
7. The Essential Diversity of Blockchain Nodes, Thomas Burke, CACI, International IEEE Blockchain Newsletter, December 2018
8. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain , Authors: Stefano De Angelis , Leonardo Aniello , Roberto Baldoni, Federico Lombardi, Andrea Margheri , and Vladimiro Sassone, Research Center of Cyber Intelligence and Information Security, Sapienza University of Rome
9. Zibin Zheng and Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang,”Blockchain challenges and opportunities: a survey, Int. J. Web and Grid Services, Vol. 14, No. 4, 2018, 352-376
10. Clique. https://github.com/ethereum/EIPs/issues/225.
11. Go-Ethereum. https://geth.ethereum.org.
12. G. Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014