Appendix K: DIDO Consensus

Return to Reference Architecture (RA) or Return to Appendices

Consensus

Return to Top

Consensus, in DIDOs, is when the entire distributed system agrees upon the state of the data within the system. In other words, the data within the entire system can be relied upon and reflects the *"truth"*. However, although the data within the DIDO is immutable, it does not mean it is static. Every proposed change in state to any data held within the DIDO is allowed when there is **Consensus** that the new data state is valid and verified.

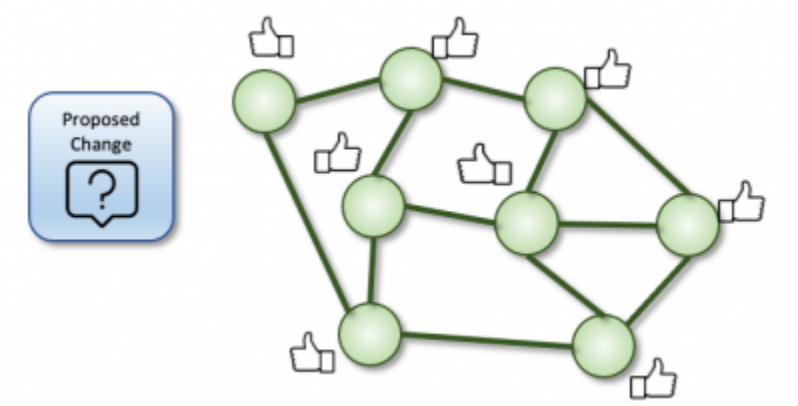

Figure 1: The DIDO Network Nodes have Consensus the data state represents *"truth"*.

Notes

Return to Top

There is a difference between a **DIDO Consensus** and a **Community of Interest (CoI) Consensus**. The **DIDO Consensus** concerns the way Consensus for propagating transactions throughout the DIDO Network. DIDO Consensus is generally inherent to the DIDO Platform. When there is a preference for a particular Consensus Mechanism for a particular project, the preference needs to be addressed as part of the functional requirements for the project.

CoI Consensus is concerned with how decisions are made in the CoI. The details of how Consensus is reached within a COI are generally captured in the Community's (i.e., Ecosphere's) Policies and Procedures (P&P).

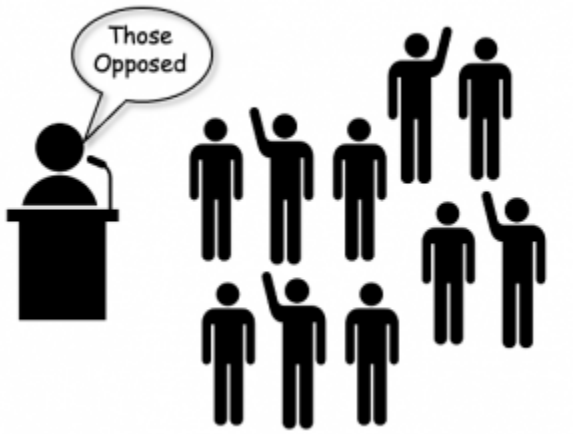

Figure 2: The COI Consensus.

- K.3 Consensus Mechanisms

Proof of Work (PoW)

Return to Top

Developed by Satoshi Nakamoto, Proof of Work is the oldest consensus mechanism used in the Blockchain domain. It is also known as mining where the participating nodes are called miners.

In this mechanism, the miners have to solve complex mathematical puzzles using comprehensive computation power. They use different forms of mining methods, such as GPU mining, CPU mining, ASIC mining, and FPGA mining. And the one that solves the problem at the earliest gets a block as a reward.

However, the process is not that easy. A puzzle can be solved only via the trial and error method. Additionally, the level of complexity of the puzzle increases with the speed at which blocks are mined. So, it becomes mandatory for one to create a new block within a certain time frame to cope up with the difficulty level.Webpage: BHARDWAJ

Proof of Elasped Time (PoET)

Return to Top

PoET was introduced by Intel with an intent to take over cryptographic puzzles involved in PoW mechanism by considering the fact that the CPU architecture and the quantity of mining hardware know when and at what frequency does a miner wins the block.

It is based on the idea of fairly distributing and expanding the odds for a bigger fraction of participants. And so, every participating node is asked to wait for a particular time to participate in the next mining process. The member with the shortest hold-up time is asked to offer a block.

At the same time, every node also comes up with their own waiting time, after which they go into sleep mode.

So, as soon as a node gets active and a block is available, that node is considered as the ‘lucky winner’. This node can then spread the information throughout the network while maintaining the property of decentralization and receiving the reward.Webpage: BHARDWAJ

Proof of Capacity (PoC)

Return to Top

Proof of Capacity (PoC), also known as Proof of Space (PoS), are solutions for every complex mathematical puzzle is accumulated in digital storage like Hard disks. Users can use these hard disks to produce blocks, in a way that those who are fastest in evaluating the solutions get better chances for creating blocks.

The process it follows is called Plotting.Webpage: BHARDWAJ

Directed Acyclic Graphs (DAG)

Return to Top

Consensus Protocol

Return to Top

Consensus Protocol, in DIDOs, is developed by a specific DIDO platform to implement **Consensus Mechanism** over their DIDO network to achieve **Consensus**.

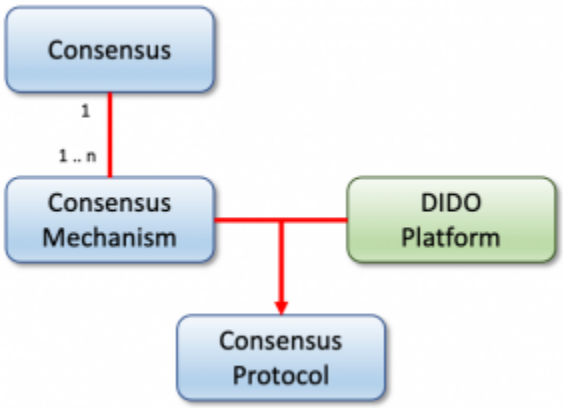

Figure 3: The relationship between Consensus, Consenus Mecahnism, and Consensus Protocol.

Transaction

Return to Top

All data within the DIDO are immutable with newer values (i.e., data states) being posted using a transaction that provides instructions on how to migrate the original data state to a new data state. Over time, the chain of history of data state changes (i.e., **Journal**) for one piece of data can become quite long. Given a known data state at a particular time, the current state of the data can be reconstructed using the journaled transactions.

In addition, the new data state also includes references back to the original data state. This allows the navigation of the journal back to the original data state (i.e., **Genesis Data**).

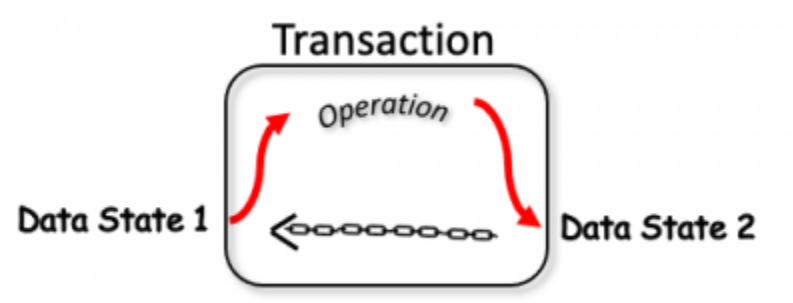

Figure 4: Transaction move the Data from one state to the next and remember the precious data state.

The following are some examples of Data State change commands. These are not Transactions because they do not include a reference to the original data to be changed (i.e., altered).

```
CHANGE EmotionState FROM HAPPY TO GLAD
CHANGE AccountBalance BY +5.00
```

- **Note:** In the example above, to be a transaction, the GLAD data state also has a reference back to HAPPY data state.

Why is it important

Consensus Algorithm are essential in establishing confidence in a DIDO.

Thus there are various types of consensus algorithms in blockchain prospect, some of them are explained below[1)]

- K.1 Definition of Terms
- K.3 Consensus Mechanisms
- K.4 Consensus Platforms
- K.5 Consensus Algorithm References
- platform

Table 1:

Consensus Alorithym	Description	Platform Examples	Pros	Cons	Type
Proof of Work (PoW)		Bitcoin, Litecoin, ZCash, Primecoin, Monero, Vertcoin	Less opportunity for 51% attack Better Security	Greater energy consumption Centralization of Miners	Competitive ConsensusWebpage: SAINI
Proof of Stake (PoS)		Ethereum, Dash, Peercoin, Decred, Reddcoin, PivX	• Energy efficient Webpage: SAINI • More expensive to attack for attackers Webpage: SAINI • Not susceptible to economies of scale Webpage: SAINI	• nothing-at-stake problem Webpage: SAINI	Competitive Consensus Webpage: SAINI
Delegated Proof of Stake (DPoS)		• Steem, EOS, and BitShares Webpage: BHARDWAJ • BitShares, Steemit, EOS, Lisk, Ark Webpage: SAINI	• Energy efficient. Webpage: SAINI • Fast. Steemit, a high traffic blogging site uses it. EOS has a block-time of 0.5 sec. Webpage: SAINI	• A bit centralized.Webpage: SAINI • Participants with high stakes can vote themselves in to become a validator. Something which is seen recently in EOS.Webpage: SAINI	Collaborative consensusWebpage: SAINI
Leased Proof of Stake (LPoS)		Waves			
Proof of Elapsed Time (PoET)		Hyperledger Sawtooth, Resource-Efficient Mining (REM)			
Practical Byzantine Fault Tolerance (PBFT)		Stellar, Ripple, Hyperledger FabricWebpage: BHARDWAJ			
Simplified Byzantine Fault Tolerance (SBFT)		Chain			

Consensus Alorithym	Description	Platform Examples	Pros	Cons	Type
Delegated Byzantine Fault Tolerance (DBFT)		NEO Webpage: BHARDWAJ			
Directed Acyclic Graphs (DAG)		Iota, Hedera Hashgraph Webpage: BHARDWAJ			
Proof of Activity (PoA)		• Espers and Decred Webpage: BHARDWAJ • Decred Webpage: SAINI			Collaborative consensusWebpage: SAINI
Proof of Indentity (PoI)					
Proof of Importance (PoI)		NEM			

Consensus Alorithym	Description	Platform Examples	Pros	Cons	Type
Proof of Capacity (PoC) Proof of Space (PoS)		Burstcoin and SpaceMint Webpage: BHARDWAJ	• Similar to PoW but uses space instead of computation. Thus much environmental friendly. • Can be used for malware detection, by determining whether the L1 cache of a processor is empty (e.g., has enough space to evaluate the PoSpace routine without cache misses) or contains a routine that resisted being evicted. • Can be used for anti-spam measures and denial of service attack prevention.	Incentivization can be an issue.	Collaborative consensusWebpage: SAINI
Proof of Burn (PoB)		Slim Coin Webpage: BHARDWAJ			
Proof of Weight (PoW)		Algorand, Filecoin, Chia	• Energy efficient.Webpage: SAINI • Highly Customisable and scalable.Webpage: SAINI	• Incentivization can be hard.Webpage: SAINI	Competitive consensus Webpage: SAINI

1)

Coinjoker, Consensus Algorithms in Blockchain, Accessed: 9 July 2021, https://www.cryptoexchangescript.com/blockchain-consensus-algorithms