DATA GUMBO

Proof of Evidence as Consensus Mechanism

The Data Gumbo Perspective

2020

INTRODUCTION

There's plenty of online fodder exploring consensus mechanisms in blockchain. As the technology provides an immutable, decentralized record of truth with no central authority, consensus protocols supply validation and verification of transactions posted and hosted on the blocks.

By definition, a consensus mechanism is "a fault-tolerant mechanism used to achieve the necessary agreement on a single data value or a single state of the network among distributed processes and multi-agent systems." Typically, there are three main types of consensus mechanisms that employ varied sets of principles:

- **Proof of Work (POW)**
  Most often invoked within popular cryptocurrency networks, this mechanism requires participants nodes to prove the work executed and then submits it for qualification to be added as a transaction on a blockchain.
- **Proof of Stake (POS)**
  A lower-cost algorithm that POW, POS allocates responsibility for maintenance in a ledger to participants proportioned by stakes held.
- **Proof of Capacity (POC)**
  In this mechanism, memory space of contribution nodes are shared among participants with a larger amount of rights granted to the larger participants.

What the above have in common are basic features to determine efficiency. These include protocols to ensure real-time value, security, and fault tolerance. Selecting the right type of consensus model for a network is dependent on considerations for that particular network including the relationship between participants and functional and/or nonfunctional aspects for complexities.

A NEW WAY: PROOF OF EVIDENCE (POE)

At Data Gumbo, we characterize our consensus algorithm in a new way, Proof of Evidence (POE), otherwise called Proof of IoT. In GumboNet™, our industrial blockchain network of suppliers, vendors and companies, nodes are authorized to agree to particular blocks being correct. Historically, the buyer's node holds authority for the correctness of each transaction but we are moving to a split-authority model where both buyer and seller have equal authority to affirm each particular transaction.

> *"In GumboNet... we are moving to a split-authority model where both buyer and seller have equal authority to affirm each particular transaction.*

CHANGING THE CONVERSATION

In addition to having only the nodes that are actually financially involved in a transaction approve it, we are changing the larger conversation around consensus algorithms, putting proof of the physical delivery of goods or services onto the blocks itself to make an auditable record of transactions, thus solving commercial transactions.

We enable businesses to create templates for their contracts that turn operational and executable aspects of a regular contract into simple code that can be automated as a smart contract depending on POE to trigger transactions. For example, if 10 tons of sand, as measured by the tare weight of the truck, is delivered at location X, the company that delivers the sand is automatically paid for the 10 tons at the pre-agreed price. Proof of the transaction, including GPS tracking of the truck and scale readings tied to the hardware ID of the controller for the scale are written to a shared ledger as evidence for the transaction in the same block that has the calculated payment.

> *“Consensus is achieved by counterparties agreeing upfront to acceptable sources of evidence, then executing transactions using streams of data, agreed business logic and the agreed price books.*

Nodes continue to compare hashes to ensure matching and a sustained integrity of records. Consensus is achieved by counterparties agreeing upfront to acceptable sources of evidence, then executing transactions using streams of data, agreed business logic and the agreed price books.

IMPLEMENTING A POE MODEL

To implement a POE model, we’ve had to make various trade offs. One is that the larger block information payloads needed to store evidence results in slower transaction speeds. In industrial use cases, executing hundreds to thousands of transactions per day per smart contract is perfectly acceptable. Since our use cases are on private ledgers between known parties with each party treated as a technical peer, there is no need for zero knowledge proofs or other exotic computing to keep validators from seeing information. In fact, the information shared is what has been contractually agreed to be shared.

Furthermore, since there is no need for cryptocurrencies in industrial use cases, we have dispensed with mining and other mechanisms built around token management entirely. The result is that parties to GumboNet smart contracts have complete transparency throughout the configuration, execution and recording of every individual transaction and can audit the code, the data and the calculated payments at any time with the data in their own copy of the ledger.

Companies are able to tie physical assets such as wells, pads, rigs, pipelines, trucks and so on directly to smart contracts. By agreeing upfront to terms and data sources to confirm the satisfaction of terms connected via standard API on those assets, smart contracts powered by GumboNet operate with a POE consensus mechanism.