Quorum Key Components

Key Components

Key concepts are developed for those who want to understand its basic architecture. It contains:

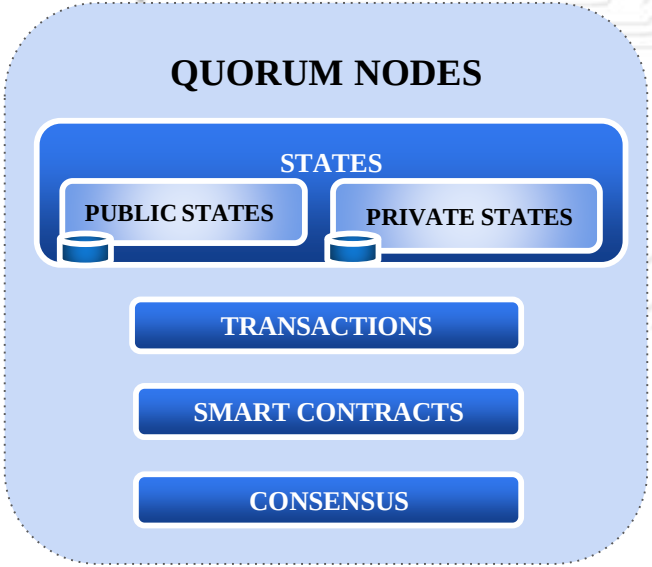
- Network
- Nodes
- States
- Transactions
- Consensus
- Constellation
- Crypto Enclave
- Transaction Manager

Quorum Network

- An Authenticated peer-to-peer network in which a node is simply a Ethereum Virtual Machine (EVM).
- Shareability on a need-to-know basis.
- The flow of all communication between nodes is straightforward. Ethereum P2P messaging protocol is used.
- Every network has a Network Manager.

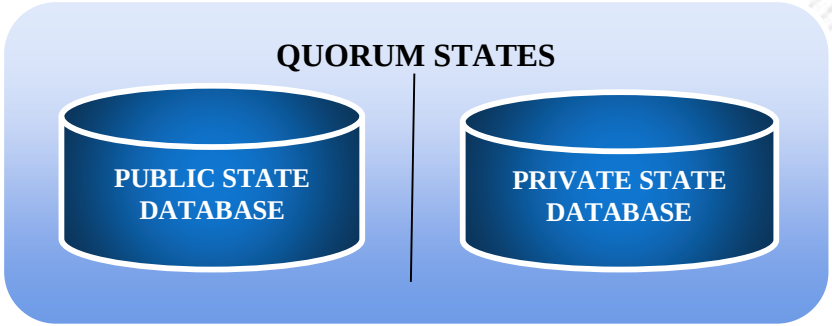
Quorum Node

- Quorum Node is a lightweight part of geth. It continues to expand with the growing Ethereum community.
- Interact with Ethereum P2P messaging Protocol.
- Hosts Quorum services and Dapps.
- Each node maintains its own *permissioned-nodes.json* file.
- State database has been split into:
  - **Public state database**
  - **Private state database.**
- No pricing of Gas.



States

- State is an immutable object that represents facts which are known by one or more nodes at a specific point of time.
- States are never altered, they are either unconsumed (unspent) or consumed (spent).
- States contain reference to contracts that govern the evolution of state.
- States maintain their own database. It is divided into two:
    - **Public State Database**
    - **Private State Database**



Transactions

- Transactions are the proposals to update the ledger.
- Quorum transaction uses the extended model of the Ethereum Transaction Model.
- Ledger evolvement happens while applying transactions.
- Quorum Transaction is propagated to the rest of the network using the standard Ethereum P2P Protocol.

Types of Transactions:

- **Private Transaction:** Transactions whose payload is only visible to the authorized network participants for that transaction.
- **Public Transaction:** Transactions whose payload is visible to all participants of the same network.

Consensus

- Consensus is the agreement that allows the nodes to choose algorithms based on their requirements in terms of privacy, scalability, legal-system compatibility, and algorithmic agility.
- Updates are applied using transactions, consuming existing state objects, and producing new states.
- No need of Proof-of-Work or Proof-of-Stake consensus algorithms.

Types of Consensus Algorithms:

- **RAFT Consensus:** Used for faster blocktimes, on-demand block creation, and transaction finality.
- **Istanbul BFT Consensus:** PBFT-inspired consensus algorithm with transaction finality.
- **Clique POA Consensus:** Default POA consensus algorithm bundled with Go Ethereum.

Constellation

- Constellation is the Haskell implementation of a general-purpose system for secure information transmission that implements a self-managing, simple peer-to-peer network.
- It is consolidation of a distributed key server, PGP encryption, and Mail Transfer Agents (MTAs.)
- Not blockchain-specific, potentially applicable to many other applications.
- It supports a number of storage backends and access controls like an IP whitelist.
- Constellation modules consist of two sub-modules:
  - **Transaction Manager**
  - **Crypto Enclave**

Crypto Enclave

- Enclave is a cryptographic mechanism used for strengthening the privacy of transactional data.
- It performs encryption and decryption of transaction data along with symmetric key generation in an isolated way.
- Crypto Enclave works hand in hand with the Transaction Manager.
- It holds private keys and is a Virtual Hardware Security Module (virtual HSM) isolated from other components.

Transaction Manager

- Transaction Manager stores and enables access to encrypted transaction data, exchanges encrypted payloads with the transaction managers of other peers.
- It is responsible for transaction privacy and managing local data stores.
- It does not have access to any sensitive private keys.
- It utilizes the enclave for cryptographic functionality.
- Stateless in nature and it can be load balanced easily.

THANK YOU!

Any questions?

You can mail us at

hello@blockchain-council.org