HYPERLEDGER FABRIC

HYPERLEDGER FOUNDATION

Hyperledger Fabric Enterprise Blockchain

Launched in 2016 and hosted by the Linux Foundation as an open-source collaborative effort to advance cross-industry Enterprise-ready blockchain technologies.

Overview: Fabric is a modular and extensible open-source system for deploying and operating permissioned blockchains. It supports modular consensus protocols, which allows the system to be tailored to particular use cases and trust models. Due to its innovative architecture, Hyperledger Fabric has the ability to deliver unique network capabilities such as enhanced privacy and confidentiality, efficient processing, scalability, standard programming languages, and a modular structure that can be customized for individual deployments. Such capabilities make Fabric a suitable blockchain platform for businesses.

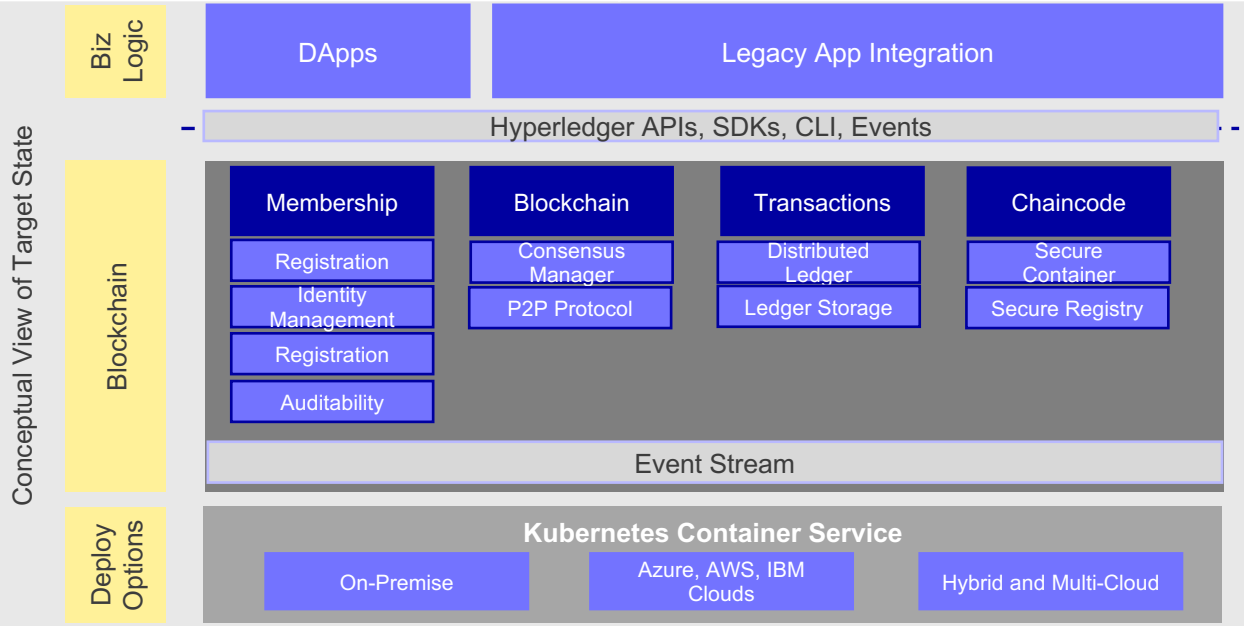
Benefits: For businesses that want to reduce the "human element" of aggregating, amending, and sharing data, Quorum will allow for less manual intervention in these processes, which will in turn provide for employees to spend more time on their actual responsibilities.

Industries: Hyperledger is used in logistics, food safety, healthcare, identity protection, IOT, property, payments, capital markets, and post trade

Customers: Walmart, Unilever, Nestle, UBS, Splunk, Honeywell, FDA, London Stock Exchange.
Competitors: Quorum, Ripple, Corda

Key Features

- Permissioned Network - Establish decentralized trust in a network of known participants rather than an open network of anonymous participants.
- Enterprise-Grade Performance – Can process hundreds of transactions per second; enough to support enterprise volumes
- Multiple pluggable consensus mechanisms are suitable for enterprise use cases.
- Token or Cryptocurrency Agnostic – Does not use crypto-assets, cryptocurrency, tokens, or coin-like constructs as incentive mechanics to establish trust systems.
- Permission Management – Limits participation to a known set of nodes that have to be provisioned to be part of the blockchain network.
- Flexible approach to data privacy: data isolation using 'channels', or share private data on a need-to-know basis using private data 'collections'
- Quarriable data (key-based queries and JSON queries)



Hyperledger Blockchain Components

- **Membership Services**- A permissioning module that acts as a vehicle to establish a root of trust during network creation. It is also instrumental in ensuring and managing the identity of members.
- **Consensus Services**- Pluggable models(e.g., RAFT, BFT) meet use case needs.
- **Assets** – Anything that holds monetary value on the system. Represented as a key-value pair on the network.
- **Chain-code Services** – Chaincode is an application-level code stored on the ledger as a part of a transaction.
- **Ledger** – Encodes the transaction history in an immutable ledger. ACL support.
- **Security and Crypto Services** –
- **APIs, Events, SDKs** – Support enterprise integrations without exposing the details of blockchain-powered business networks.

Hyperledger works with existing Tools and Ethereum

- Build on Languages – Java, Node.js, Go
- Deploy – Jenkins, Docker, Terraform, Kubernetes
- Monitoring – New Relic, Azure Monitor, AWS Cloudwatch, Stackdriver, Nagios, Bitnama
- Support for EVM and Solidity

Security & Privacy

- Permissioned Network – Pluggable membership identity service to manage the identities in the permissioned network.
- Data and Privacy Controls – Ability to set privileges on which nodes can see assets and transactions.
- Infrastructure – Flexible deployment options allow for greater oversight of network and application control.
- Non-interactive Zero-Knowledge Proofs – Prevents unauthorized peers from accessing channel resources.
- Digital Signatures – Fabric relies on PKI for digital signatures and the digital identities that are perilous to the operational security of its network.
- GDPR Compliant – Consistent methods deployed to protect each user's PII
- Not Post-Quantum Secure – Information that is shared over the network is vulnerable to malicious decryption techniques by large-scale quantum computers. However, Fabric provides a pluggable cryptographic provider that enable quantum security.

Hosting

- Microsoft Azure
- AWS
- GCP
- IBM
- Oracle

Quorum | CONSENSYS | Microsoft Azure

Quorum Enterprise Blockchain

Consensys acquired Quorum from JP Morgan in 2020. It replaces Microsoft's Blockchain service (retired in 2021).

Overview: Quorum is an enterprise grade blockchain platform. It is a fork of the public Ethereum client 'geth' with several protocol level enhancements to support enterprise needs. The primary purpose of the Quorum platform is to enable an enterprise Ethereum client which empowers businesses to embrace and benefit from blockchain technology.

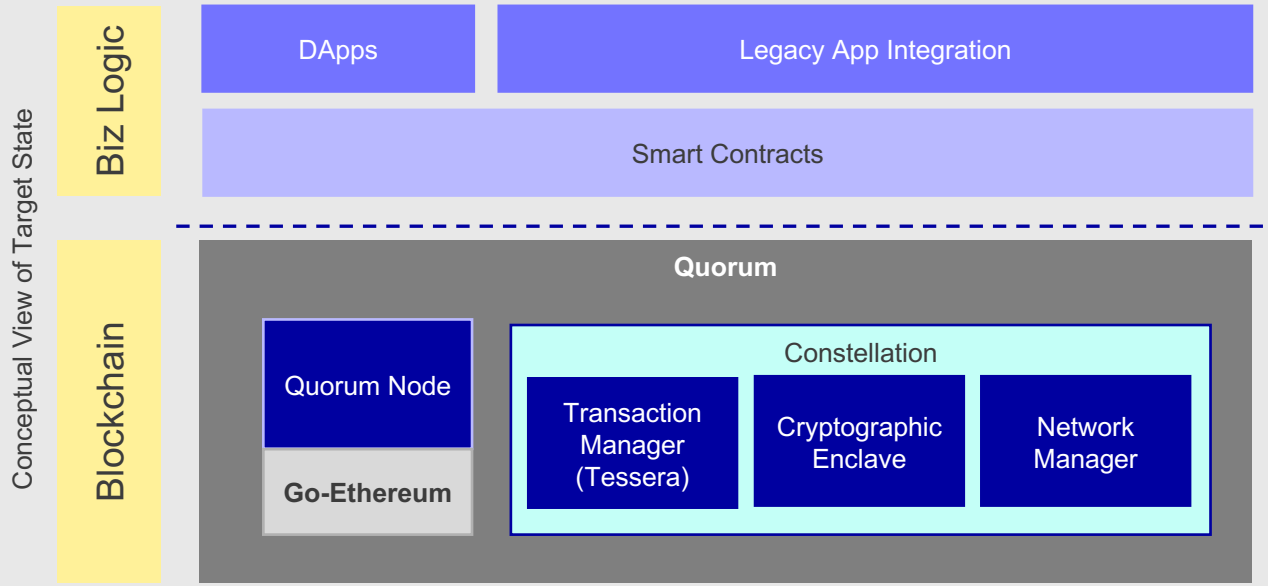
Benefits: For businesses that want to reduce the "human element" of aggregating, amending, and sharing data, Quorum will allow for less manual intervention in these processes, which will in turn provide for employees to spend more time on their actual responsibilities.

Industries: Quorum is used in logistics, healthcare, identity protection, property, payments, capital markets, and post trade

Customers: JP Morgan Chase , Ant Group, ING Group, LVMH, HSBC, Novartis, Cargill, Microsoft
Competitors: IBM Hyperledger Fabric, Corda

Key Features

- Transaction Privacy - Stores vanilla Ethereum transactions as well as hashes of encrypted private smart contract state changes.
- Uses Advanced encryption techniques - Ensures only permissioned entities can access the network.
- Enterprise Grade Performance – Can process hundreds of transactions per second; enough to support enterprise volumes
- Multiple pluggable consensus mechanisms suitable for enterprise use cases.
- No Transaction Pricing – No need for Ether/Gas to execute transactions.
- Permission Management – Limits participation to a known set of nodes that have to be provisioned to be part of the blockchain network.



Quorum Blockchain Components

- **Transaction Manager** - allows access to encrypted transaction data for private transactions, manages local data store and communication with other Transaction Managers
- **Crypto Enclave** - responsible for private key management and encryption and decryption of private transaction data
- **Quorum Node** - voting-based, BFT-hardened consensus mechanism that utilizes core Ethereum features to verify and propagate votes through the network
- **Network Manager** - controls access to the network, enabling a permissioned network to be created
- **Constellation Network** – Private Smart contracts transmitted point to point so that only relevant parties receive them.

Quorum works with existing Ethereum Tools

- Truffle Testing Framework
- Metamask Wallet and Gateway
- OpenZeppelin – Modular Reusable Smart Contracts
- Remix

Security & Privacy

- Permissioned Network – Known Peers Only
- Quorum offers decentralized privacy - No dependency on a central node/service or external application to ensure privacy
- Single-chain architecture - Chain contains both public & private transactions guarantees privacy whilst ensuring better security
- Designed to meet regulatory requirements around in-country data & is compatible with next gen crypto primitives such as ZKP
- Leverages Baseline Protocol (using Zero-Knowledge Proofs) to allow access to public Ethereum network while keeping transactions private.
- Not Quantum Secure – Future Pluggable Consensus methods will eventually provide support.

Hosting

- Microsoft Azure
- AWS
- Google Cloud
- On-Premise