Experiment No. 8

Aim:

Case Study on Other Blockchain platforms

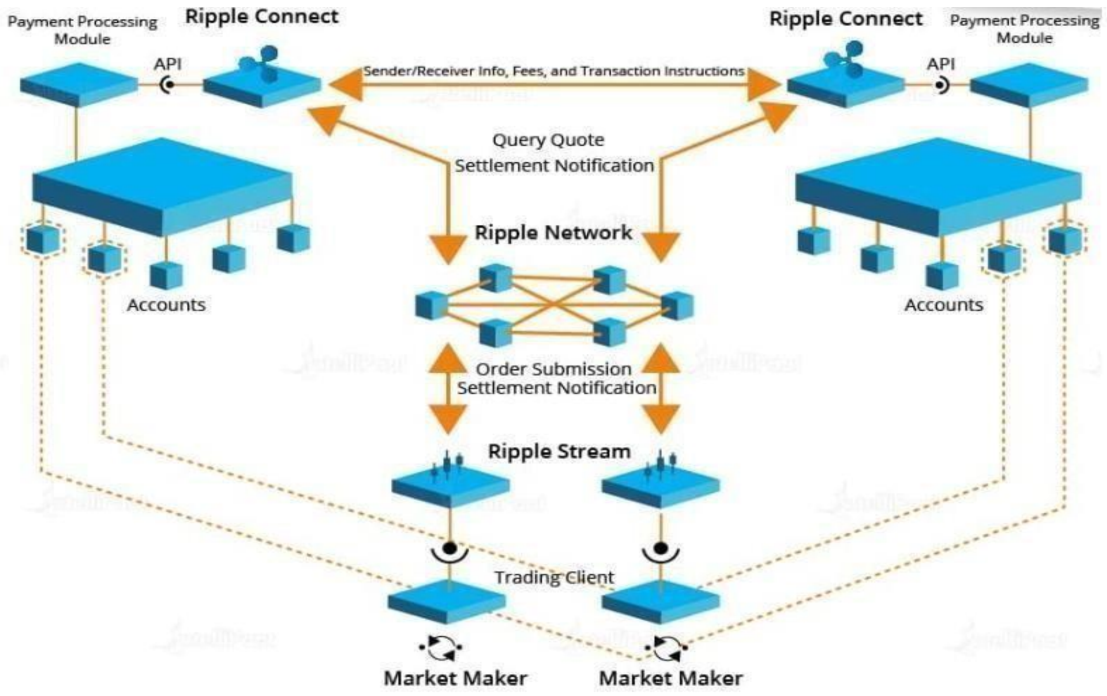
Theory:

Ripple: Ripple is an open-payment network for digital currency. It is also a holding company. Ripple is a privately held cash flow positive company that aims to create and enable a global network of financial institutions and banks to use ripple software, to lower cost of international payments. It is also cost-efficient and real-time enabled. Ripple calls this global network using ripple software products. The Ripple (XRP) ledger is an open-source product created by ripple.It was created to reduce major points of friction in international payments.

XRP can be used by banks to control liquidity on demand in the real time. XRP pays providersto expand into new markets, provide faster payment settlement and lower foreign exchange cost. Unlike Bitcoin, ripple aims to work with current financial world, the equivalent of roughly 155 trillion of dollars move across the board every year. Ripple uses what it calls gateways, which are similar to global ledger, made up of something similar to private blockchain. This is essentially a digital portal that government companies and financial institutions use to join the ripple network. This is called a ripple transaction protocol or ripple net.

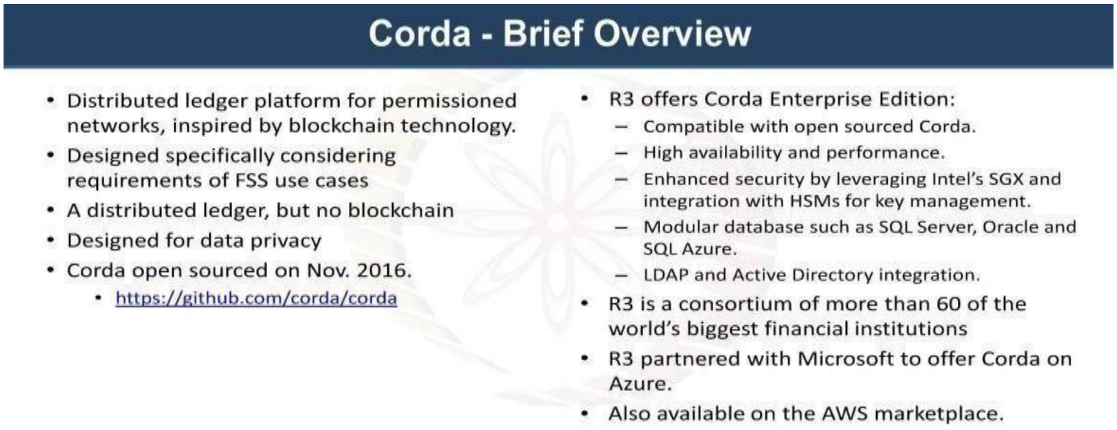
Network members process payments through a product called as "xCurrent". It provides pre-validation of transactions and rich data attachments for repayment. It also provides payment certainty through pre-disclosure of information to eliminate failures. It also enables atomic settlement and updates pass/fail status across all intermediaries.

Network members can also source on demand liquidity through the product "xRapid", which provides access-on-demand liquidity through digital assets. It provides lower liquidity costs through on-demand liquidity sourcing. It reduces the need for nostro accounts to make global payments. The product titled "xVia" is a standard API-based interface to access the Ripple Network. Global payments can be made with certainty through this API as it can access across networks to make on-demand and real-time payment. It also enables rich data attachments along with end-to-end visibility.



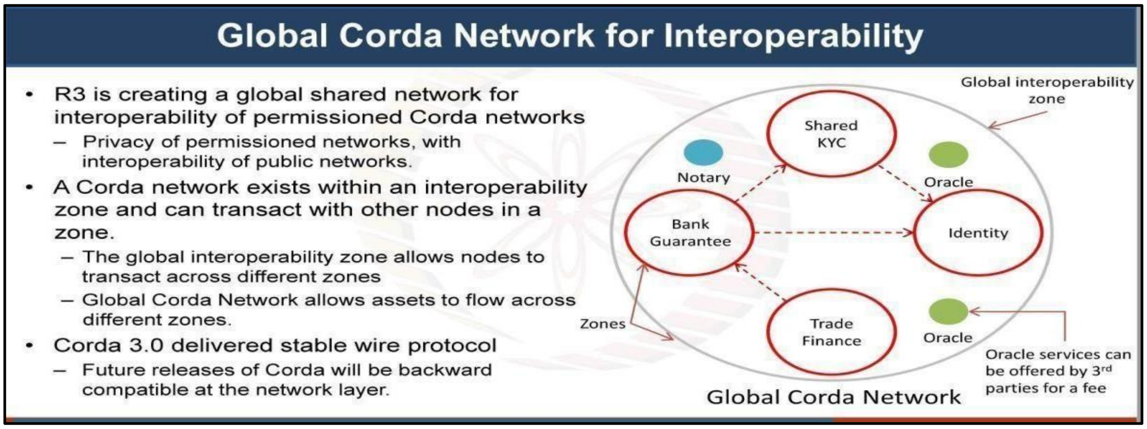
Fund Transfer in a Ripple Blockchain System

Corda: Corda is another open-source distributed ledger technology (DLT) and was developed by R3, which is a consortium of more than 200 companies like Amazon, Microsoft, and Intel. It has built-in app programs for various domains and industries (DApp), like Banking, (around 150 banks are part of it). It works on the principle of need-to-know basis, shared ledger, and isnot a gossip network. Based on the need-to-know principle, only necessary information is shared with the relevant stakeholders. Information will not be shared with everybody. Corda isfreely availablein the internet and anybody can use it. Following are the four characteristics of Corda: Need to know, Interoperability, Shared ledger, Smart contacts.



Corda - Brief Overview

- Distributed ledger platform for permissioned networks, inspired by blockchain technology.
- Designed specifically considering requirements of FSS use cases
- A distributed ledger, but no blockchain
- Designed for data privacy
- Corda open sourced on Nov. 2016.
  - https://github.com/corda/corda
- R3 offers Corda Enterprise Edition:
  - Compatible with open sourced Corda.
  - High availability and performance.
  - Enhanced security by leveraging Intel's SGX and integration with HSMs for key management.
  - Modular database such as SQL Server, Oracle and SQL Azure.
  - LDAP and Active Directory integration.
- R3 is a consortium of more than 60 of the world's biggest financial institutions
- R3 partnered with Microsoft to offer Corda on Azure.
- Also available on the AWS marketplace.



Global Corda Network for Interoperability

- R3 is creating a global shared network for interoperability of permissioned Corda networks
  - Privacy of permissioned networks, with interoperability of public networks.
- A Corda network exists within an interoperability zone and can transact with other nodes in a zone.
  - The global interoperability zone allows nodes to transact across different zones
  - Global Corda Network allows assets to flow across different zones.
- Corda 3.0 delivered stable wire protocol
  - Future releases of Corda will be backward compatible at the network layer.

Quorum Blockchain:

Quorum is an "Enterprise-focused" Ethereum blockchain that tries to improve blockchain technology. Although the first generation Blockchain provides scalability, peer-to-peer networks, interoperability, transparency, and other features, it is still not perfect. Researchers around the world are working hard to improve the state of the blockchain. Quorum is the brainchild of JP Morgan, which developed to advance blockchain technology in the financial industry.

Need For Quorum

At present, the finance sector's information is handled by more than one organization, but still,the finance sector suffers from a lack of transparency, information control, and security. The traditional blockchain also does not fulfill the finance sector requirements even if it provides traceability and immutability. There is a need for a system that provides private control on the blockchain through automation which is customizable according to needs.

Features of Quorum

- **Performance:** Quorum is faster than Bitcoin and Ethereum. It carries out more than 150 transactions per second. This is because of the simple consensus mechanism used by quorum. By default, quorum uses RAFT consensus for fault- tolerance and IBFT consensus for Byzantine fault tolerance, which is quite faster than Ethereum's proof ofwork consensus.
- **Permission Management:** It limits participation to a known set of nodes that haveto be provisioned to be part of the blockchain network, so it is not open to all and implemented only between participants that are pre-approved by a designated authority
- **Elimination of transaction pricing:** It eliminated the concept of adding cost to a transaction using gas. There is no need for any cryptocurrency costs associated with running transactions on the quorum network. The Quorum code was initially forkedoffEthereum, the usage of the gas itself exists but is set to zero.
- **Better Privacy:** Quorum provides on-chain public and private transactions. The open transactions are similar to Ethereum, whereas private transactions are not exposed to the public. It uses Constellation technology which encrypts specific messages in a place called an enclave and stores information about previous transactions.

- **Assets Management:** It allows an entity to create, manage, and distribute digital assets without going through a third party. This gives the owner autonomy over howtomanage their assets.
- **Open Source:** It is an open-source where more than 300 contributors are active and working on the development of Quorum.

Quorum Architecture:

The architecture is shown below in Diagram 1.

It consists of Quorum node, Privacy manager, Transaction manager, Enclave

- **Quorum node:** The Quorum node is a lightweight fork of geth**.** The consensus is achieved with RAFT, PoA or Istanbul BFT consensus algorithms instead of using Proof-of-Work. Block validation logic has been modified to handle ‘Private Transactions Transaction creation has been modified to allow for Transaction data to be replaced by hashes of the encrypted payloads in order to preserve private data where required. The pricing of Gas has been removed, although the Gas itself remains.

Quorum supports both public and private transactions. Public transactions work normally as in public ethereum where private transactions are enabled through a separate component called private transaction manager (privacy manager).

Privacy manager : The privacy manager component (private transaction manager) is responsible for providing transaction privacy on the Quorum network. In other words, this component allows Quorum nodes to share transaction payload securely between authorised parties of the transaction. It consists of two sub elements, namely the transaction manager and enclave.

Transaction manager : It is a restful and stateless service which is primarily responsible for the following operations.

- Automatic discovery of the other transaction manager nodes on the network
- Exchanges encrypted payloads with other nodes’ transaction managers
- Stores and allows access to encrypted transaction data

Enclave: Distributed Ledger protocols typically leverage cryptographic techniques for transaction authenticity, participant authentication, and historical data preservation

Advantages of Quorum:

- **Consensus Algorithm:** It uses the “Quorum-Chain” consensus algorithm which is based on majority voting. However, not all nodes are capable of voting. Only a few and selected nodes are given the ability to vote in the voting process. This helps in the verification of the transaction. Quorum uses Istanbul BFT and Raft- based models for better fault tolerance. Only selected participants take part in the network.

- **Hybrid Smart Contracts:** Smart contracts are set to both private and public and solidity is used to program them. Once a smart contract is set private, it cannot be transformed into a public one.

Similarly, public smart contracts cannot be changedto private ones, which makes them more secure.

- **Performance:** Quorum provides higher transaction speed since generally private contracts are used and private contracts work better than public ones. It has been tested that the Raft performs better than the Istanbul BFT.

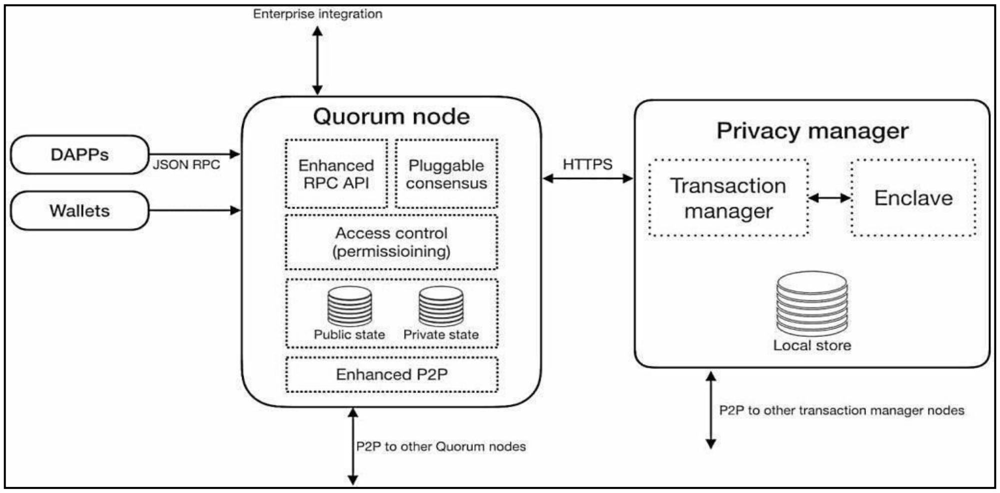
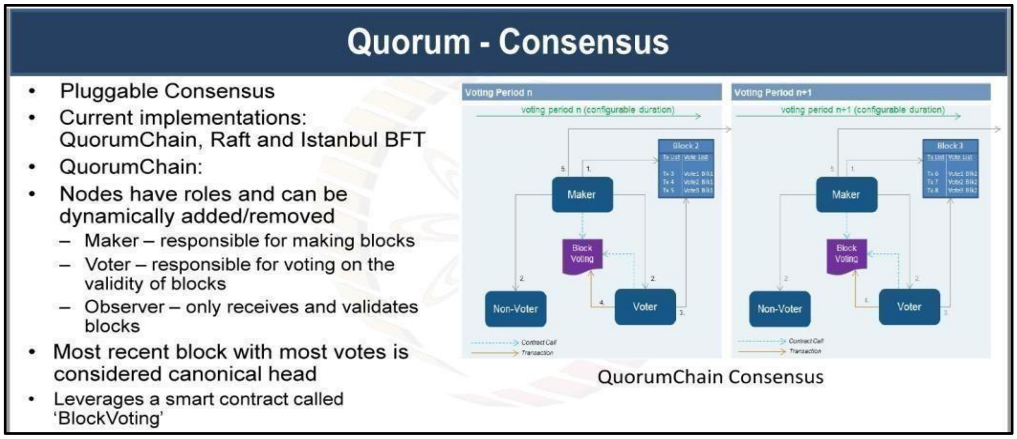


Fig. 1 Quorum high level architecture



Quorum - Consensus

- Pluggable Consensus
- Current implementations: QuorumChain, Raft and Istanbul BFT
- QuorumChain:
- Nodes have roles and can be dynamically added/removed
  - Maker – responsible for making blocks
  - Voter – responsible for voting on the validity of blocks
  - Observer – only receives and validates blocks
- Most recent block with most votes is considered canonical head
- Leverages a smart contract called 'BlockVoting'

QuorumChain Consensus

Disadvantages of Quorum:

- **Scalability:** Quorum's channel-based approach to privacy presents challenges for privacy and scalability as use cases become more complex.
- **Lack of crypto-economics**: Quorum doesn't require a built-in cryptocurrency because consensus is not reached via mining. It's not possible to develop a native currency or a digital token with Quorum.
- **Lack of Support:** There are fewer developers and contributors to Quorum, due to which the help and support are less.

Conclusion:

Q. Can you provide a case study of a company or organization that implemented a blockchain platform other than Ethereum or Hyperledger and detail the benefits they achieved?