IT Fundamentals

Assignment 3

Author: Melvin Mokhtari

Student ID: 9831143

Instructor: **Dr. Mohammad Hossein Manshaei**

Date Last Edited: June 6, 2022

Quorum is an open-source blockchain protocol that was developed specifically for usage in a private blockchain network. A single member owns all the nodes, or a consortium blockchain network, where multiple members each own a portion of the network. J.P. Morgan first announced it in 2017 and has been actively developing it ever since.

Fundamentally, Quorum is the public Ethereum client, which is enhanced with enterprise features. It provides privacy features, enterprise permissions, and improved performance in a permissioned network. A component called the Private Transactions Manager serves as an off-chain privacy mechanism.

Here is how Quorum is different from the Ethereum Blockchain:

One of Quorum's most distinguishing features is that it is a permissioned system, meaning that the Quorum network will not be accessible to everyone. Only authenticated and authorized users have access to this network. The trade between players in Quorum is pre-approved by a specified authority; the system has a permissioned chain of people in it.

One of the critical features that banks look at is the confidentiality of data. We utilize the existing Blockchain or Ethereum technology, which does not ensure data security. Because visibility and ease of access are critical aspects of blockchain, banking and financial institutions are hesitant to use this technology. When it comes to Quorum, its permissioned nature makes it a good idea. It describes the difference between public and private transactions. Open transactions are comparable to Ethereum, but private transactions are private, and data is not visible to the public. One of the key features which makes Quorum superior to Ethereum or other blockchain platforms is Constellation. It is one of the essential features of Quorum. It secures the messages by enslaving them. In this enclave, there are previous transactions' authenticity and authentication. Most cryptographically heavy work relies on it, thus making it a secure and safe mechanism.

Quorum is based on the QuorumChain voting consensus mechanism. The functioning of this consensus mechanism is straightforward; it delegates voting rights to others. To assign voting rights, QuorumChain makes use of smart contracts. It not only assigns the voting rights but, at the same time, also tracks the status of all the voting nodes.

It is far superior to its contemporaries when it comes to the speed of transactions in Quorum. As per the development team, the system can easily handle more than 100 transactions per second, which is higher than Bitcoin and Ethereum. As a result, Quorum is the preferred choice for banking and other financial institutions. Such high speed is its simple consensus mechanism, which allows quicker transactions.

In 2019, JP Morgan Chase, the owner of Quorum, introduced a coin called JPM to facilitate value transfers between companies using Quorum. JPM is a stable coin pegged to the US dollar. Still, due to its private and commissionable nature and the fact that the bank verifies the transactions, many within the community believe that the JPM coin does not fit the criteria of a cryptocurrency.

The JPM Coin enables the instantaneous transfer of payments between institutional accounts. This means only selected miners will be able to process transactions, unlike in public cryptocurrencies where anyone can.

Quorum uses the RAFT consensus for fault tolerance and the IBFT consensus for Byzantine fault tolerance, which is faster than Ethereum's proof-of-work consensus.

Like Ethereum, Quorum is a fully EVM-compatible distributed ledger and supports intelligent contracts to create programmable applications and related units of value. The smart contract languages supported by Quorum are Solidity and Vyper.

Quorum supports privacy features to allow confidential transactions, including transfers and smart contracts, to cater to business needs. Quorum, which was built as a "consortium chain," extends the Ethereum Transaction Model to account for new transaction privacy characteristics.

At the transaction level in Quorum, a distinction between public and private status is established:

- Regular Ethereum transactions are characterized as public transactions. Any node can read them, including the payload and additional data.

- Private transactions enable parties to conceal the content of transactions from the rest of the network by including a dedicated parameter that includes a list of public addresses that can see the payload.

Quorum, unlike Ethereum, uses a Proof-of-Authority algorithm. Quorum supports three algorithms:

- Raft-based: A consensus model for faster block times, transaction finality, and on-demand block creation.

- Istanbul BFT (Byzantine Fault Tolerance): A consensus algorithm inspired by PBFT with immediate transaction finality.
- Clique POA Consensus: A default POA consensus algorithm natively supported by the go-Ethereum library.

Transaction ordering in this blockchain is also covered. Synchronization between the leader and other nodes in Raft ensures that the order of transactions is consistent across all nodes before they are executed. In IBFT, each transaction in the blockchain follows a single, agreed-upon order.

Consensus	Description	Fault tolerance	Forkable
Raft	Nodes follow the block leader in this leader/follower process; they only mint blocks if at least one transaction is in a block. Fast block times are best if there is no fear of malicious behavior from parties.	Up to 2f+1 nodes can be tolerated by the Istanbul BFT, where f is the number of faulty nodes.	Not possible
Istanbul BFT	Multiple rounds of voting by the group of validators are used to reach a mutual consensus. It is possible to make empty blocks. If there is a threat of malevolent action from third parties, this is the best option.	Up to 2f+1 nodes can be tolerated by the Istanbul BFT, where f is the number of faulty nodes.	Not possible
Clique POA	Signers (”approved accounts”) validate transactions and blocks. Signers take turns creating the next block. Empty blocks can be produced. However, it may result in forks.	Up to 2f+1 nodes can be tolerated by Clique POA, where f is the number of faulty nodes.	Possible

The significant distinction between Raft and any other Crash Fault Tolerance algorithm is that Raft followers believe in their leader ultimately.

In IBFT, however, each block requires multiple rounds of validator voting to obtain a mutual agreement, which is then recorded as a collection of signatures on the block content. As a result, IBFT is slower than Raft.

Quorum is used for tokenization, copyright protection, supply chain management, energy and commodity trading, and provenance for industry focus.

This private blockchain explorer is called Epirus, and it is a dockerized environment designed to view private Quorum networks.

So, to put it in a nutshell, Quorum specifications are listed in the table below:

Cryptocurrency	JPM coin, but there are no monetary expenses connected with using the Quorum network.
Consensus Protocols	Raft, IBFT, Clique POA
Ledger Type	Private, Permissioned
Industry Focus	Cross-Industry
Smart Contract Functionality	Yes
Smart Contract Languages	Solidity, Vyper
Version	Peer: 2.7.0; Transaction manager: Tessera 0.10.6
Explorer	Epirus

Stellar is an open-source payment system that resembles Ripple in numerous ways. Jed McCaleb, the company's founder, was also a co-founder of Ripple.

Stellar is a payment tool that aims to connect financial institutions and substantially lower the cost of transfers. At first, both payment networks utilized the same protocol.

Even before Ethereum, Stellar was launched in 2014. Stellar is considered a dinosaur by some in the crypto sector.

Stellar is a payment mechanism based on distributed ledger technology. It permits cross-border transactions between any currency pair in a matter of seconds. In many aspects, it resembles other blockchain-based cryptocurrencies.

"A technology that connects banks, payment systems, and people," according to its website, "to transfer money quickly, reliably, and at almost no cost."

The original digital currency of Stellar, Stellar Lumen (XLM), is utilized to power the blockchain network's entire range of operations. At the start, 100 billion XLM were created.

Inflation is the only other way to create XLM. Economic growth and lost Lumens are accounted for by a 1% yearly inflation rate on the Lumen creation rate. Fresh Lumens are manufactured and distributed every week using a direct voting system.

Like those on any other blockchain platform, transactions on the Stellar network are recorded in a shared and distributed public ledger. Stellar employs the "Stellar Consensus Protocol" (SCP), a consensus mechanism based on the Federated Byzantine Agreement (FBA).

The Stellar Consensus Protocol uses federated voting to guarantee safety and liveness. The goal is to conduct several federated votes on multiple values until one passes through SCP's various voting phases, which are detailed below.

The values on which SCP seeks consensus could be stellar ledgers or lunch orders, but it is critical to emphasize that these are not the values on which SCP's federated-voting rounds vote, accept, or confirm. Instead, federated voting takes place on statements that express such beliefs.

In the nomination phase, the initial rounds of federated voting take place on a family of statements of the type "I nominate V" for various V values. The purpose of the nomination is to identify one or more such assertions that can be accepted and confirmed.

Following the confirmation of confirmable candidates, SCP moves on to the balloting step, where the goal is to locate a ballot (a container for a nominated value) and a quorum willing to commit to it. If a quorum agrees to vote on this ballot, the result of the consensus round determines the value of the vote. However, before a node can vote to commit to a ballot, it must first confirm that all lesser ballots are aborted. These steps—aborting ballots to find one that can be confirmed committed—involve multiple rounds of federated voting on multiple statements about ballots.

SCP allows for faster transactions at lower costs by allowing everyone on the network to agree on the authenticity of a transaction in seconds. Each participant (referred to as a node) who assists in adding transactions to the global ledger chooses a mini-network of other trusted participants. "Quorum Slices" are the names for these mini-networks.

Compared to the decentralized proof-of-work and proof-of-stake algorithms, SCP has modest financial and computing requirements, reducing entry barriers and opening up the financial system to new participants.

As long as Quorum Slices overlap, the Stellar network can quickly reach a consensus on legitimate transactions and add them to the ledger.

Stellar, specializing in sending, storing, and trading value, lacks a smart contract language and a built-in virtual machine to run code.

Stellar Smart Contracts (also known as SSCs) combine transactions with various constraints to get a result. Constraints that can be coupled to form SSCs include the following:

- Multisignature: Multiple parties must sign transactions on an account in order for it to be multisig. You may also set signature thresholds and weights.
- Batching/Atomicity: The concept of batching entails combining numerous actions into a single transaction. Atomicity is the promise that if one operation fails in a set of operations, they will all fail.
- Sequences: Sequence numbers are used to represent things in Stellar. If an alternative is submitted, sequence numbers can be used to influence transactions and guarantee that certain transactions will fail.

- Time bounds: Time boundaries are limits on how long a transaction can be valid, and they can be used to represent time in Stellar smart contracts.

Due to these limits, SSCs have a smaller scope than Ethereum smart contracts, but they can still be used for escrow contracts, joint entity lightning channels, crowdfunding, and other innovative uses. You can also write them in your preferred programming language, reducing the number of flaws and possible assaults.
Another significant distinction between SSCs and Ethereum smart contracts is that the smart contract's conditions and logic are generated independently of Stellar and then published to the network as a transaction once the end conditions are met. You are not directly dealing with code on-chain as a participant in a Stellar smart contract, but instead agreeing to the terms of a transaction.
Assume Alice wishes to commission Bob to create a work of art. They agree that if Bob completes the art piece in 30 days, Alice will pay him $100. However, if it takes longer, Alice will only have to pay $60. Alice might then establish a transaction for both end circumstances using an escrow account, multi-signature, and/or time-bounds. The escrow account could subsequently be handed on to a trustworthy third party. When the work of art is completed, the responsible party submits the transaction to the end condition (whether it was completed in 30 days or not) to the network. Bob gets his money, and Alice has to pay for the correct final result.
USDC, WXT, GTN, SIX, NWC, SHX, MOBI, TFT, REPO, RIO, and UVU are some examples of cryptocurrencies on the Stellar Blockchain.
Stellar's essential operation is similar to that of most decentralized payment technologies. It runs on a network of decentralized servers with a distributed ledger that is updated every 2 to 5 seconds among all nodes and can work on both public and private ledgers.
Stellar allows you to produce, send, and trade digital representations of any currency, including dollars, pesos, bitcoin, and almost anything else. It is designed so that all the world's financial systems can work together on a single network.
So, to put it in a nutshell, stellar specifications are listed in the table below:

Cryptocurrency	USDC, WXT, GTN, SIX, NWC, SHX, MOBI, TFT, REPO, RIO, UVU
Consensus Protocols	Stellar Consensus Protocol (SCP)
Ledger Type	Both public and private
Industry Focus	Financial Services
Smart Contract Functionality	Yes & No!

- Please check this link for the video explaining and codes of the ”Make a Simple Blockchain” question.