MODULE 6:

TOOLS AND APPLICATIONS OF BLOCKCHAIN

Prepared By: Prof. Swapnil S. Sonawane

HYPERLEDGER FABRIC

Hyperledger Fabric is an open source, permissioned blockchain framework, started in 2015 by The Linux Foundation.

It is a modular, general-purpose framework that offers unique identity management and access control features, which make it suitable for a variety of industry applications such as track-and-trace of supply chains, trade finance, loyalty and rewards, as well as clearing and settlement of financial assets.

How does Hyperledger Fabric Work?

1. The transaction flow begins when a client application sends a transaction proposal to peers in each organization for endorsement.
2. The peers verify the submitting client's identity and authority to submit the transaction. Next, they simulate the outcome of the proposed transaction and if it matches what was expected, it sends an endorsement signature back to the client.

3. The client collects endorsements from peers, and once it receives the proper number of endorsements defined in the endorsement policy, it sends the transaction to the ordering service.
4. Lastly, the ordering service checks to see if the transaction has the proper number of endorsements to satisfy the endorsement policy. It then chronologically orders and packages the approved transactions into blocks and sends these blocks to peer nodes in each organization. Peer nodes receive new blocks of transactions from the ordering service, and then do a final validation for transactions in that block. Once this is complete, the new block is added to the ledger and the state of the ledger is updated. The new transactions are now committed.

Advantages:

Open Source:

Hyperledger Fabric platform is an open source blockchain framework hosted by The Linux Foundation.

Permissioned:

Fabric networks are permissioned, meaning all participating member’s identities are known and authenticated.

Governance and Access Control:

Fabric networks consist of channels. Members on the network can transact in a private and confidential way. Each transaction on the blockchain network is executed on a channel, where each party must be authenticated and authorized to transact on that channel. This provides an additional layer of access control and is especially useful when members want to limit exposure of the data

Performance:

Hyperledger Fabric is built to support enterprise-grade use cases, and can support quick transaction throughput from its consensus mechanism

CORDA

Corda is a distributed ledger platform designed to record, manage and automate contract based legal agreements between two or more parties.

As in Blockchain which embodies the Distributed Ledger Technology (DLT), the data are stored in all the nodes in the blockchain making it highly secure.

This means that an individual or any entity outside the block can never change the data for their own agenda.

This makes it highly secure but at the same time raises the issue of the number of files and the space it takes up.

Smart contracts play a vital role in blockchain, i.e., the contract would be transparent and accessible by everyone in the block. But the main difference with Corda, is that the smart contract can be permission based.

Only the two or more parties involved in the transaction would have access to the smart contract. Also, with the consensus of the parties involved, a regulatory or a legal body or notary can be given access and brought into the network as an observer to verify the contract.

Advantages of Corda:

Data and transaction privacy:

Corda is very flexible when it comes to private transacting. You can assign public or private status to different transactions based on the specified business rules.

Fast operational speeds:

A key element of how Corda achieves good transaction speeds is its unique transaction verification model. On most blockchains, transactions are accumulated into a block, hang in the waiting mode while the block is being filled, and only then get the chance to be verified. On Corda, each transaction is sent to verification immediately, i.e., verification happens at the individual transaction, not the block level.

Optimizing the costs and efficiency of inter-company cooperation:

By creating a blockchain-based network on Corda, businesses can significantly improve cooperation efficiency and cut down on the cost of interacting.

RIPPLE

Ripple is a blockchain-based digital payment network and protocol with its own cryptocurrency, XRP.

Rather than use blockchain mining, Ripple uses a consensus mechanism, via a group of bank-owned servers, to confirm transactions.

Ripple transactions use less energy than bitcoin, are confirmed in seconds, and cost very little, whereas bitcoin transactions use more energy, take longer to confirm, and include higher transaction costs.

Ripple (XRP) ranks among the most valuable blockchain-based tokens by market capitalization.

The Ripple payment system is intended to be used primarily by banks, but individual investors can speculate on the price of XRP.

Working of Ripple:

1. The XRP crypto uses a consensus protocol to confirm transactions.
2. Validators compare proposed transactions to the most recent version of the XRP ledger to determine whether they are valid.
3. The majority of validators must accept a transaction to be verified.

How Is Ripple Mined?

Ripple (XRP) is created using a crypto ledger with blockchain technology

1. While it is true that miners cannot mine Ripple (XRP), it is technically viable to do it using other cryptocurrencies.
2. Mining Bitcoin (BTC) and Ethereum (ETH) and then exchanging the mined coins for Ripple (XRP) through exchanges is one of the most effective methods for mining XRP.

QUORUM

Quorum is an “Enterprise-focused” Ethereum blockchain that tries to improve blockchain technology.

Features of Quorum:

Performance: Quorum uses RAFT consensus for fault-tolerance and IBFT consensus for Byzantine fault tolerance, which is quite faster than Ethereum’s proof of work consensus.

Elimination of transaction pricing: It eliminated the concept of adding cost to a transaction using gas.

Assets Management: It allows an entity to create, manage, and distribute digital assets without going through a third party.

Better Privacy: Quorum provides on-chain public and private transactions. The open transactions are like Ethereum, whereas private transactions are not exposed to the public.

Quorum Nodes:

1. Quorum Node: It is a lightweight fork of Geth. It is configured only to allow connection from permission nodes, ditching the P2P connectivity.
2. Constellation: It kept the transaction manager and enclave. It ensures that information added to the blockchain remains secure in every possible way.

    a. Transaction Manager: It ensures that the transaction data is encrypted during the process by storing the allowed access and other important data to facilitate the transactions.

    b. Enclave: It provides different cryptographic techniques such as participant authentication, transaction history, and other key functions to ensure that all the operations are performed optimally with a focus on scalability.

Advantages:

Consensus Algorithm: It uses the “Quorum-Chain” consensus algorithm which is based on majority 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.

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 changed to 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 BFT.

DEFI

Decentralized finance, or DeFi, uses emerging technology to remove third parties and centralized institutions from financial transactions.

The components of DeFi are stable coins, software, and hardware that enables the development of applications.

Working of DeFi:

Users typically engage with DeFi via software called dapps (“decentralized apps”), most of which currently run on the Ethereum blockchain. Unlike a conventional bank, there is no application to fill out or account to open.

Here are some of the ways people are engaging with DeFi today:

Lending: Lend out your crypto and earn interest and rewards every minute - not once per month.

Getting a loan: Obtain a loan instantly without filling in paperwork, including extremely short-term “flash loans” that traditional financial institutions don’t offer.

Trading: Make peer-to-peer trades of certain crypto assets — as if you could buy and sell stocks without any kind of brokerage.

Saving for the future: Put some of your crypto into savings account alternatives and earn better interest rates than we typically get from a bank.

Buying derivatives: Make long or short bets on certain assets. Think of these as the crypto version of stock options or futures contracts.

Advantages of DeFi:

Open: You don’t need to apply for anything or “open” an account. You just get access by creating a wallet.

Pseudonymous: You don’t need to provide your name, email address, or any personal information.

Flexible: You can move your assets anywhere at any time, without asking for permission, waiting for long transfers to finish, and paying expensive fees.

Fast: Interest Rates and rewards often update rapidly (as quickly as every 15 seconds) and can be significantly higher than traditional Wall Street.

Transparent: Everyone involved can see the full set of transactions (private corporations rarely grant that kind of transparency)