Blockchain Platforms - Key Takeaways

Below you will find a number of key points from this course. Defined terms are underlined.

Week One: Permissioned Blockchains

Permissioned Blockchain allows only nodes with permission to transact and take part in the blockchain operations.

Permissioned blockchain is also known as a consortium blockchain based on its common usecases in specific vertical business domains such as the auto or food services consortiums.

Linux Foundation's Hyperledger is an ecosystem supporting not only blockchain protocols but it also supports the framework and tools for active engagement and collaboration of developers, businesses and other stakeholders.

The goal of the Hyperledger Project is to promote the development of a safe, reliable, efficient, innovative, quality-driven, open-source components and platforms to support enterprise adoption of the blockchain technology.

Hyperledger has **five** frameworks: Fabric, Sawtooth, Indy, Iroha, and Burrow

There are no cryptocurrency In the **Hyperledger** protocol

Chaincode is the smart contract code in Hyperledger that defines a set of assets and provides the functions for operating on the assets and changing their states. It also implements application specific rules and policies.

Hyperledger Fabric is a permissioned business blockchain

Here is the list of services offered by the Fabric:

1. Identity services
2. Policy services
3. Blockchain services and
4. Smart contract services

Identity services module manages the identities of entities, participants, and ledger objects such as smart contracts. In the case of Fabric it is called chaincode.

Policy services module manages access control, privacy details, consortium rules and consensus rules.

Blockchain services module manages

- the peer-to-peer communication protocol,
- distributed ledger maintaining the global state,
- global state replicated at many participants, and
- pluggable consensus algorithm (PBFT, or POW)

Smart contracts services module provides a secured and lightweight sandboxed environment for the chaincode to execute.

APIs allow application programs to call into the underlying services. **SDKs** help in code development based on these APIs. **CLI** is the command line interface for invoking these APIs for testing purposes.

Peers are nodes that initiate transactions and maintain the state of the ledger. There are three types of peer nodes:

1. **Endorsing peers** receive and validate transactions, sign them, and return them to the creating application. They are called endorsers.
2. **Ordering peers** collect signed transactions, order them into blocks, and send them to the committing peers. This is also known as ordering service.
3. **Commiting peers** receive the blocks created by ordering service, validate conditions such as double spending and signatures, and then commit them to the ledger.

Channel provides segregated fabric for a group of entities to transact privately. Channels also provided the ability to support multi-lateral transactions among competing businesses and regulated industries through cross-chain chaincode.

An **identity** determines the role of the entities and the permissions they have for accessing the resources in the blockchain network.

Consensus is the agreement on the next block of transactions to be added to the chain and the extensive validation and verification of the order and correctness of the transactions including double spend and other conditions.

Microsoft Azure's main goal is to accelerate blockchain deployment. Azure BaaS features include:

- A Collection of ready to deploy ledgers
- Blockchain network with multiple nodes, with hashing, mining, the consensus among the nodes, and the distribution of replicated ledger to all nodes
- Preconfigured network configurations for developing business logic
- Tools and infrastructure in a single place
- Data security and scalability of the cloud platform and
- Single Node Ledger and Multi Node Ledger

Week Two: Decentralized Application Platforms

Augur is a trustless, decentralized prediction market platform based on blockchain technology.

Roles participants can play in the prediction market:

1. Market creator who places the prediction query, sets the expected outcomes, pays fees and escrows, establishes the rules, and designates the initial set of reporters.

2. Trader who places the bets on the expected outcomes and takes part in the pre-reporting phase of the process. Traders buy and trade shares that bet on the odds of the outcomes. The trading currency is currently ETH.

3. Reporter who reports on the outcomes. Understand that outcomes do not have to be binary (Yes or No). The reporter can be a designated reporter or an open reporter based on the phase of the process.

Grid+ is a Dapp platform implemented on Ethereum blockchain that has created an energy ecosystem by integrating blockchain and AI.

Energy Retailer: Grid+ will operate as a commercial electricity retailer in deregulated markets.

Smart Agent: At the user household, Grid+ smart agent is a computing device that hosts the software for the blockchain transactions, multi-signature crypto-wallet, with PKI security and off-chain payments for faster confirmations.

Intelligent electricity usage: Electricity trading is a complicated process with many intricacies; Grid+ manages these by coding the efficient price options using smart software.

ERC-20 Token payments: A special ERC20 compliant token called BOLT has been created for payment purposes.

Integration to IOT devices: A Smart agent can be integrated into other intelligent agents such as NEST and electric batteries (Telsa Powerwall)

Remote control: Grid+ enables integration of mobile phones and computing devices to allow remote control of its operation.

Week Three: Challenges and Solutions

In **Proof of Stake (POS)**, the full node with the most at stake or most coins is chosen for adding the next block. That is why is it is called Proof of Stake. The idea is that the node with most at stake will not be malicious and risk its stake for forking the network.

In **Practical Byzantine Fault Tolerance (PBFT)**, nodes vote to elect a leader, and that leader adds the next block to the chain. This leader adds the block of validated transactions.

Scalability is the ability of a system to perform satisfactorily at all practical levels of load. Load in the context of the blockchain could be: transaction times, number of nodes, number of participants and accounts, and other attributes of the blockchain.

Escrow is “a contractual agreement in which a third party receives and disburses money or documents for the primary transacting parties, with the disbursement dependent on conditions agreed to by the transacting parties..”

Week Four: Alternative Decentralized Solutions

IPFS is a decentralized model for file transfer in contrast to the centralized namespace and transfer provided by the http family of protocols.

Bitswap protocol manages the block exchanges involving the nodes accordingly.

Hashgraph is a trust model that provides a consensus layer that addresses the transaction latency, and energy wastage, fairness and also provides a computationally strong algorithm for Byzantine Fault Tolerance, and eventual consistency. Forks are mechanisms that add to the robustness of the Blockchain framework.

Elements of the hashgraph include:

- Event
- Transactions
- Directed acyclic graph: DAG The hashgraph
- Witness
- Famous Witness
- Round: Round Created, Round Received
- Consensus by voting by the witnesses of the next round and
- Gossip protocol

A **round** consists of all the events between the oldest participant and youngest participant of the round.

Bitcoin has had a butterfly effect on technology, its concept has opened up a Pandora's box of technology and efforts ushering in a technological and possibly a social “revolution.”