**Lecture 7 Notes**

Slide 4

* It is a closed ecosystems that can only be accessed by those who are allowed access.
* Anyone who is interested in validating transactions or viewing data on the network needs to get approval from a central authority.
* Ripple, Hyperledger are the perfect examples of a permissioned blockchain.
* Permissioned governance is also known as private governance ― it restricts access in terms of who can perform various actions on a blockchain.
* Transactions are validated and processed by those who are already recognized by the ledger and some level of pre-existing trust is assumed and proven.
* The internal mechanics of a permissioned blockchain can vary, from existing participants serving as a type of administrator who decides on the inclusion of future entrants to simple observers, but essentially a permissioned blockchain can’t be accessed by the general public.
* There are many examples of permissioned blockchains, like [Quorum](https://github.com/jpmorganchase/quorum), a distributed ledger protocol with transaction and contract privacy created by JPMorgan and [Corda](https://www.corda.net/),
* an open-source blockchain designed for businesses to transact directly between one another in strict privacy.
* The security on private blockchains is only as good as the honesty of the entities validating transactions, i.e. a company.
* There are no mathematical guarantees behind the irreversibility of transactions in a private blockchain.
* However, they still use cryptography and data structures to maintain integrity.

Slide 5

* a permissioned Blockchain, Hyper- ledger has been developed for a variety of networks. Hyper- ledger [10] introduces six business frameworks: Fabric,
* Burrow, Iroha, Sawtooth, Indy, and Quilt. Depending on tech- nological requirements and wide variety of consensus algo- rithm [12], different frameworks can be utilized. Hyperledger
* Fabric can be used as a foundation for developing Blockchain solutions targeted for IoT network. The basic components of a permissioned Blockchain architecture has been shown in
* Fig. 1. BC network is formed through interconnection of peers, where peers are independent servers. They are responsible for validation and endorsement of transactions, and maintain
* the distributed ledger. Validation and endorsement process are mostly dependent on smart contract (chaincode) which must be installed on every endorsing peer. Basically, smart contract
* is a programmatic code to deﬁne the transaction rule or policy in between sender and receiver. Successfully endorsed transactions are stored as a block into a common ledger which
* is integrated with peers. Many transactions may ﬁt into a single block which must be linked with the last block of the ledger by hash value, which makes a chain of blocks

Slide 6

* While permissionless blockchains are increasingly gaining acclaim in the world of business, many firms are now beginning to take cognizance of the many upsides to adopt blockchains to augment their systems.
* They do this to instill trust, transparency, and, in the case of B2B exchanges, efficiency.
* For example, the Hyperledger Foundation is the pioneering open-source initiative for B2B blockchains.
* In a permissioned blockchain, the showrunners are members of a consortium, and stakeholders opt-in to create a network.
* Pre-approved entities are the only ones who can run the node which validates transaction blocks and execute blockchain-based smart contracts.
* With permissioned blockchains, it is easy to share trusted information in a secure context.
* This is done with the confidentiality that businesses require to operate at top effort.
* A permission blockchain is designed to make use of computationally inexpensive consensus algorithms.
* Compared to permissionless relatives such as the proof-of-work, this blockchain sits on substantially better scalability and performance.
* Blockchains such as the Hyperledger Fabric have additional innovations in the offing with respect to the roles of the nodes.
* Generally, they do not use crypto-economic models or monetary tokens because of the nature of the business networks.

Slide 7

* **Governance And Transparency**
* The semantics of management are very different when it comes to the permissioned and permissionless blockchains.
* In the former, governance is determined and consented by the members of the blockchain business network.
* Among peers, code quality, code changes economic incentives, and power allocation are dependent on the dynamics of the business.
* These parameters are also based on the collective motive for which the network was formed and designed.
* This way, companies will be able to do things quickly in ways suitable for their models.
* For permissioned blockchains, having transparency into the work carried out by each node may not be as essential as it is to the network members in the permissionless sect.
* Everything is contingent on the way the business relationships are established as well as how the blockchain is configured.
* Being that a good number of permissioned blockchain networks do not have crypto-economic incentives built into them,
* the major incentives of the participants is minimizing cost, time, and the ease of sharing information across the platform.
* **Decentralization**
* For a permissioned blockchain, the degree of decentralization is dependent on how the members of the network agree to structure their business relationships.
* The ‘no central control’ concept is relevant in this case, given that the consortiums are managed entities.
* In the same way, the degree and quality of decentralization on the network rests on the number of peers, the anticipated number of bad nodes in the network, and the caliber of consensus the members decide to use.
* Algorithms such as Byzantine Fault Tolerance - which is different from the conventional proof-of-work algorithm used in permissionless blockchains - seem to be the go-to for permissioned networks.
* Hyperledger Fabric supports almost a dozen consensus algorithms via its plug-in architecture. Decentralization is a given in the design of the blockchain,
* but having the right governance model is more important.
* It is more important because power and control structures may not be evenly distributed.

Slide 8

* The architecture of a permissioned blockchain consists of Application layer, Consensus layer, and Storage layer.
* The application layer of a permissioned blockchain, similar to permissionless blockchains, consists of end-users who submit their transactions to the blockchain through a client library.
* However the consensus layer which is mainly re-sponsible for ordering and validating the transactions differs from the consensus layer in permissionless blockchains.
* In fact, since the nodes in a permissioned blockchain are known and identiﬁed, mining can be replaced with traditional consensus protocols in order to establish a total order on the requests [16].
* Finally, the storage layer, similar to permissionless blockchains, consists of a decentralized distributed ledger maintained by every node within the block-chain.
* The consensus layer runs a consesus protocol among the computing nodes of the consensus layer.
* Consensus protocols employ State Machine Replication (SMR) technique to replicates data, e.g. ledger, over nodes.
* State machine replication is a technique for implementing a fault-tolerant service by replicating servers [33].
* In the state machine replication model replicas agree on an ordering of incoming requests.
* To establish consensus among the nodes in a permissioned blockchain, asynchronous fault-tolerant protocols can be used.
* Nodes in a permissioned blockchain might crash or maliciously behave.
* In a crash failure model, nodes operate at arbitrary speed, may fail by stopping, and may restart, how-ever, they may not collude, lie, or otherwise, attempt to sub-vert the protocol.
* Whereas, in a Byzantine failure model, faulty nodes may exhibit arbitrary, potentially malicious, behavior.
* Crash fault-tolerant protocols guarantee safety in an asynchronous network using 2f+1 nodes to overcome the simultaneous crash failure of any f nodes while in Byzantine fault-tolerant protocols, 3f+1 nodes are usually needed to provide the safety property in the presence of malicious nodes.
* Permissioned blockchain mainly follow an order-execute paradigm where a set of peers (might be all of them) validates the transactions,
* agrees on a total order for the trans-actions,
* puts them into blocks and multicasts them to all the nodes.
* Each node then validates the block, executes the transactions using a” smart contract”, and updates the ledger

Slide 9

* The Blockchain concept works by creating a unique chain of blocks, with each one being “glued” to the next one by a digital signature system.
* In the context of the banking industry, this may allow checking the history of a digital value and its associated transaction records.
* Blockchains prevent actively counterfeited transactions, fraud, and collusion between rogue actors and allow a better, faster, and more efficient Know-Your-Customer (KYC) process.
* For instance, such technology may also allow interaction with other blockchains like identity blockchains provided by the public sector.
* Here is the main lifecycle of a transaction in a permissioned blockchain system: