**Lecture 6 Notes**

Slide 4

There exist 4 different types of blockchain network are

* Public
* Private
* Consortium
* Hybrid

Slide 5

* Public blockchains are permissionless blockchains where anyone can join the network and read and write to the ledger.
* Such blockchains allow users from anywhere in the world to interact with the blockchain and submit or read transactions as far as they are connected with the blockchain network.
* In a permissionless blockchain, any user can develop and add smart contracts to blockchain without any intervention forced by developers.
* Permissionless blockchains bring **complete decentralization**,
* which means that there exists no central authority to edit the ledger state or make any kind of modifications to the network protocols.
* This makes the system robust against a single point of failure with distributed trust.

Slide 6

* *How it works?*
* *Blockchain* has enabled a new wave of technological progress that can disrupt many industries and systems before us.
* The ability to seamlessly secure data in a fully transparent
* and verifiable way through a decentralized system
* That has captured the attention of people and businesses alike,
* prompting many to jump on board the bandwagon in search for a better alternative.
* Transactions on a *public blockchain* are publicly transparent and immutable
* but this could pose as a barrier for businesses that want to keep customers’ data confidential.
* On the other hand, *private blockchains*are much faster and scalable, but it is more centralized and could be prone to manipulation.

Slide 7

* Public blockchain networks like Bitcoin, Ethereum, LiteCoin, Ripple etc., are based on trustless peering.
* This means any system with public IP, beefy hardware and highspeed internet can join these networks and synchronize the entire blockchain history.
* Public blockchain reaps its benefits in the areas where network needs decentralization with anonymous access to ledgers.
* With the addition of each node, the complexity of cryptographic hashing increases
* It will lead to additional CPU usage, power, and transaction time, in order to arrive at a consensus.

Slide 8

Now, let understand bitcoin blockchain in a more detailed way:

* Imagine two friends living far away and would like to transfer money using blockchain technology
* The blockchain is a decentralized system of secure and trusted distributed databases
* Which records and shares the transaction details across many nodes(computers) so that the data is not modified
* In simple terms, a chain of blocks that contain information is called blockchain
* When a transaction occurs, its related information is recorded into a block

Slide 9

* Permissioned blockchains do not allow any user to freely join the network and read or write to the ledger.
* It maintains an access control mechanism between the list of users connected to the network
* Blockchains can be partly decentralized or fully centralized as the users have the right to do negotiation and reach a consensus with desired **varying decentralization.**
* **I**n private blockchains, users’ identity is known to everyone but transactions are only visible to those who have appropriate permission.

Slide 10

Private

* While transparency and anonymity is the support of the public blockchain,
* this is unacceptable for private corporations, especially those with financial institutions, where security is the top concern.
* Private blockchain is based on trusted peering,
* where there is no necessity for crypto-currency or mining.
* Instead of allowing anonymous connections,
* a private blockchain allows predetermined nodes to control the transactions.
* The protocols and governance of these nodes is authorized by consortia.
* This control secures sensitive data in a private blockchain and provides a deterministic latency to the transactions.

Slide 11

Example

* Hyperledger Fabric 1.0 was developed by a Hyperledger consortium,
* Joining the consortium will allow the member corporations to join the Hyperledger global network
* It allow them to collaborate with industry experts across the globe.
* IBM currently offers a Beta program to get started on Hyperledger Fabric.
* Hyperledger Fabric’s modular architecture processes a transaction in three phases.
* First, a transaction from DAPP goes through “endorsing peers.”
* Then this module processes the read-only transactions and builds datasets by executing custom business rules via smart contracts.
* These datasets are transformed into blocks by the ordering service.
* Finally, “committing peers” validate and commit the block to the ledger.

Slide 12

* A consortium blockchain is a semi-decentralized type where more than one organization manages a blockchain network.
* This is contrary to what we saw in a private blockchain, which is managed by only a single organization.
* More than one organization can act as a node in this type of blockchain and exchange information or do mining.
* Consortium blockchains are typically used by banks, government organizations, etc.
* The consortium blockchain is a hybrid between the ‘low-trust’ offered by public blockchains and the ‘single highly-trusted entity’ model of private blockchains.
* Its characteristics are the following:
* the consortium is permissioned: it’s not for everyone, but for a predetermined group of enterprises;
* it is semi-decentralized: under the supervision of members of the limited group;
* it has a multi-party consensus: all operations are verified by special pre-approved nodes, not by the world community, like in bitcoin blockchain.
* The governance roles and operating rules emergence in consortium blockchain are exhibited in the picture below.
* This slide shows how a consortium forms.
* Someone (consortium promoter) decides that there is a reason for the consortium to form.
* Once this happens founding members and participation members join with different benefits or tiers of benefits based on the operating rules of the consortium agreement which are decided by a governance board.
* These rules include such things as legal and structural decisions of the consortium as well as decisions
* which are to be implemented on the shared ledger based on a specific technology implemented by the consortium promoter with input from all of its members.
* The smart contract system and the rules engine have ensure consistency between real world contracts and smart contracts.
* **Examples** of consortium blockchain are; Energy Web Foundation, R3, etc.

Slide 13

* Hybrid blockchain offers the benefits of both public blockchain and private blockchain.
* Firstly, hybrid blockchain consists of the public blockchain and a private network that restricts participation to those invited by a centralised body.
* Secondly, this private network generates the record (hash) of transactions which is stored and verified on the public blockchain.
* The benefits of the private blockchain include faster transaction speeds, privacy of the data/ content and a centralised control over providing access to the blockchain.
* Hybrid provides an enterprise-ready blockchain solution
* that is much better suited to highly regulated enterprises and governments as
* it enables them to have the flexibility and control over what data is kept private versus shared on a public ledger.
* Coupled with the operational needs of faster transaction times, security and auditability features
* that are not suited to public blockchains.
* **Example** of a hybrid blockchain is Dragonchain.