**Lecture 2 Notes**

Slide 4

* Blockchain technology has come a long way.
* Satoshi Nakamoto wanted to create a peer-to-peer electronic cash system that did not need a network of banks to operate.
* Satoshi described “blocks” and “chains” as a way of organizing and securing records,
* such that once entries had been made into a shared database,
* they could be proved mathematically correct and to have remain unchanged.
* Blockchain software becomes the trusted record-keeping systems,
* and the rules programed into the software become the intermediaries.
* It is important to note that blockchains can be used for more than just recording the transfer of value between two parties.

Slide 5

There exist several Key components of blockchain, Few important components we are discussing here are Nodes

* Transactions
* Cryptocurrency
* Tokens
* Public Ledger
* Peer to peer Network

These are the very important keywords, So we will discuss one by one in detail.

Slide 6

* A computer connects to a blockchain network, the computer becomes a node.
* A node runs the blockchain software for the network and
* it keeps the network healthy by engaging in the transfer of information.
* Anyone can run a node on a public network like Bitcoin.
* Nodes broadcast bitcoin transactions to other nodes throughout the network and not all nodes are the same.

See the picture which shows the task and content which can be stored At Node

Node should solve typical mathematical problem to become miner and to add his block to blockchain

Any node who is part of the blockchain can validate the transactions

History of the blockchain and public ledger will be stored in the node

Slide 7

Generally there exist 3 types of nodes in the blockchain network are

* Full Node
* Light Node
* Miner Node

Slide 8

Now we will discuss one by one

First is Full Node

* A full node is a node that downloads all blocks and transactions to its local storage

More specifically, a full node,

* Has all blocks and transactions
* Full node Is a fully independent node on a blockchain network
* Full node Is able to provide blocks and transactions to other nodes
* Full node Is able to get new blocks and transactions from other nodes
* Full node Is able to verify all blocks

A full node does not need to,

* Have a pair of private/public keys. This is a misunderstanding that a full node must have a pair of private/public keys.
* A pair of private/public keys are used for signing new transactions or receiving transactions,
* which means sending or receiving coins on a cryptocurrency network.
* If your full node is only used to get all blocks and transactions for reviewing,
* then you don’t need to have a pair of private/public keys.
* However, most full nodes generate private/public key pairs automatically, regardless they are used or not.
* We also call full nodes wallets when full nodes are used on a cryptocurrency network for sending and receiving coins.

Run PoW (Do mining)

* This is another misunderstanding. PoW is an algorithm used in Bitcoin 0.1 to confirm transactions by finding a hash that meets defined difficulty (number of leading zeros).
* We call this process mining. Originally, mining was done by Bitcoin software on CPU.
* But, because the rewards generated from mining incite more people to do mining and to find faster ways of doing mining,
* So, bitcoin software runs PoW on CPU is not an efficient way of mining. Eventually, the mining feature was removed from Bitcoin software.

Slide 9

**Second node is Light Node**

* Light Node is also called Light Client and Lightweight Client.
* The benefit of a full node is that it downloads all blocks and transactions, so it is an independent node on a Blockchain network.
* The drawback of a full node is that it downloads all blocks and transactions, so it requires a lot of local storage and requires a lot of computing power to verify blocks.
* At the moment of writing, Bitcoin Core required 173 GB of local storage to store blocks and transactions of the Bitcoin network.
* The size of blocks and transactions is still growing quickly due to the heavy use of Bitcoin.
* Getting all blocks and transactions is unnecessary for people who just want to send or receive coins.
* They don’t care about old transactions.
* They don’t care about other people’s transactions.
* They only care for their own transactions.
* Therefore, Light Node was invented to save space and computing time.
* A light node only downloads block headers to validate the authenticity of the transactions.
* A light node uses a method called Simplified Payment Verification (SPV) to verify transactions.

a light node,

* Has block headers and some transactions
* Has a pair of private/public keys
* Uses SPV to verify transactions

A light node does not

* *Connect to a blockchain network directly:* A light node relies on a full node to connect to a Blockchain network.
* *Verify all blocks:* A light node relies on a full node to verify all blocks.

Because a light node is heavily relying on a full node,

the full node can see the transactions and balances of the light node.

This drawback can be remedied by connecting your light nodes to your own full node.

Slide 10

**Next node is Miner**

* Miner is a computer that helps in creating blocks for a Blockchain network.
* Originally, mining was done by a full node with full node software, such as Bitcoin.
* Because the mining process takes a lot of CPU power, so developers changed it to use GPU.
* After sometime, GPU was not fast enough, so some people come up with FPGA (Field Programmable Gate Array) mining.
* Again, FPGA was not fast enough, so the mining process is done on ASIC (Application Specific Integrated Circuits).
* Currently, ASIC is the dominant way of mining.
* The mining function is removed from the latest version Bitcoin Core software because it is useless compared with ASIC miner.
* Bitcoin ASIC is an integrated circuit specialized for Bitcoin mining. It runs specifically in mining software.

Slide 11

In terms of where and how mining is done, there are the following types of miners,

* *Solo Miner*: Solo miner is an individual miner that connects with a blockchain network directly.
* *Pool Miner*: A group of miners work together to create blocks.
* *Cloud Miner*: Mining hardware is placed in data centers. The mining capacity is sold to people who want to mine.

The figure in this slide shows 2 types of Miners with other type of full and light nodes.

Here we can c pool Miner in downside and Cloud miner on the upside,

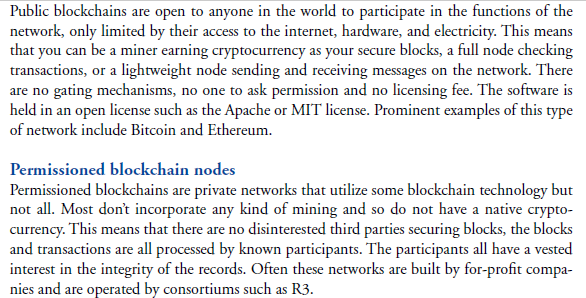
Middle there exist so 3 full nodes and one light node.

Slide 12

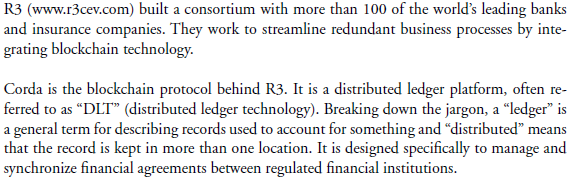
There exist other kind of nodes with respect to blockchain Architecture models and Development platforms are.

* + - Public
    - Blockchain Nodes
    - Permissioned blockchain nodes
    - Nodes on a Corda Network
    - Nodes on Hyperledger Fabric Network
    - Federated Blockchain Nodes

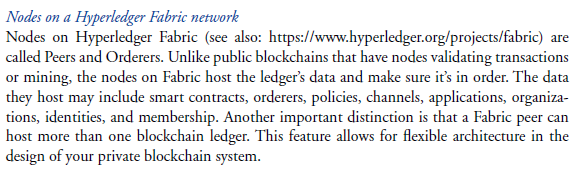
Slide 13 and Slide 14



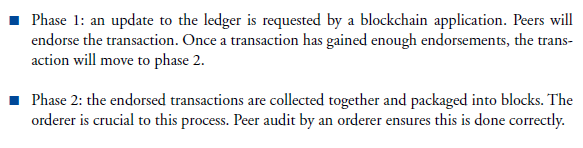
Slide 15

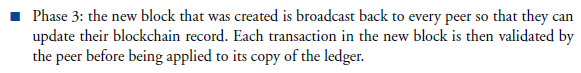


Slide 16

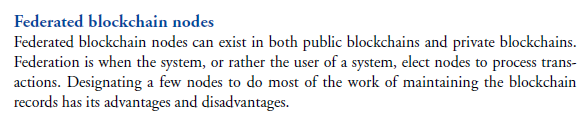


Single peer can not update the ledger by themselves



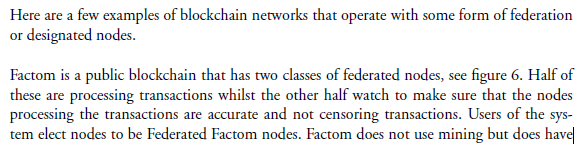


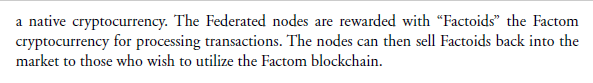
Slide 17



It reduces cost of processing transaction

It increases the blockchain updating and transaction clearance speed.





Slide 18

