Duong Quang Minh – Hoang Lan

HCMUS -  FIT

[Tiêu đề phụ của tài liệu]

## VNUHCM – University Of Science

**Information Technology (High – Quality Program)**

**Seminar - Projects**

ETHEREUM SWITCHES TO PROOF-OF-STAKES CONSENSUS

# Knowledges Engineering Seminar

**Lecturers:**

**Mr. Ngo Minh Nhut**

**Mr. Le Long Quoc**

**Semester 3 – December 1, 2022**

**Index**

1. [Personal Information 3](#_bookmark0)
2. [Blockchain 3](#_bookmark1)

[What’s blockchain ? 3](#_bookmark2)

[Key elements of a blockchain 3](#_bookmark3)

[How does blockchain work ?](#_bookmark3) 4

[Advantages of disadvantages of blockchain](#_bookmark3) 4

1. [Ethereum](#_bookmark4) 6

[**What is Ethereum ? 3**](#_bookmark5)

**Ethereum switches to PoS** [**4**](#_bookmark6)

* 1. Consensus Mechanism 5
  2. [Proof of Work 4](#_bookmark7)
  3. [Proof of Stakes 5](#_bookmark8)
  4. [The Merge 6](#_bookmark9)

1. [Demo 7](#_bookmark11)
2. [References 7](#_bookmark11)

## Personal Information

o **Name: Hoang Lan**

o **Student ID:** 1916050

o **Name: Dương Quang Minh**

o **Student ID:** 1916053

## Blockchain

### What’s Blockchain

**Blockchain defined:** Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

### Key Elements of a Blockchain

#### Distributed ledger technology:

All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that’s typical of traditional business networks.

#### Immutable records:

No participant can change or tamper with a transaction after it’s been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

#### Smart contracts:

To speed transactions, a set of rules — called a [smart contract](https://www.ibm.com/topics/smart-contracts) — is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more

### How does blockchain work ?

#### As each transaction occurs, it is recorded as a “block” of data

Those transactions show the movement of an asset that can be tangible (a product) or intangible (intellectual). The data block can record the information of your choice: who, what, when, where, how much and even the condition — such as the temperature of a food shipment.

#### Each block is connected to the ones before and after it

These blocks form a chain of data as an asset moves from place to place or ownership changes hands. The blocks confirm the exact time and sequence of transactions, and the blocks link securely together to prevent any block from being altered or a block being inserted between two existing blocks.

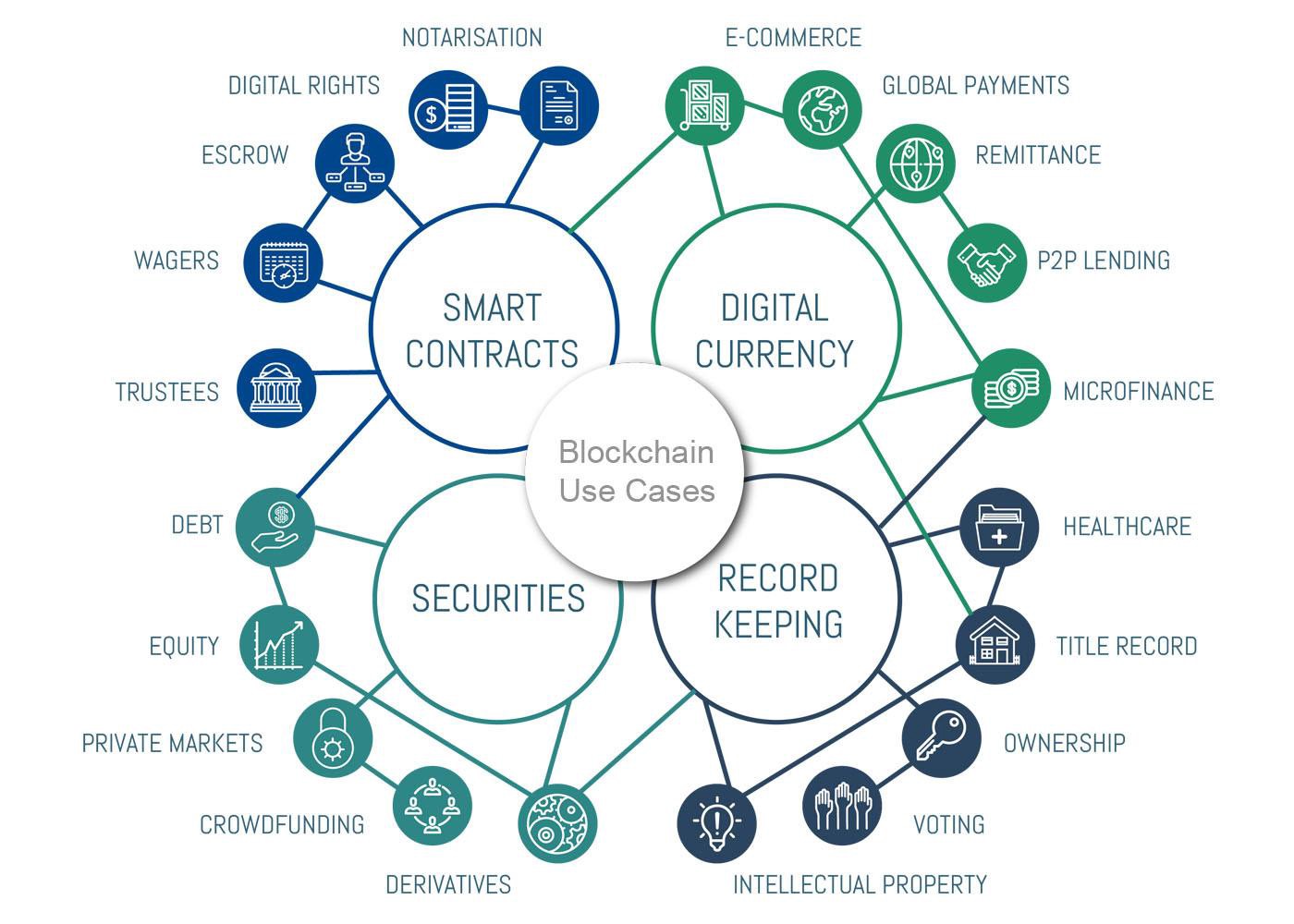
#### Transactions are blocked together in an irreversible chain:a blockchain

Each additional block strengthens the verification of the previous block and hence the entire blockchain. This renders the blockchain tamper-evident, delivering the key strength of immutability. This removes the possibility of tampering by a malicious actor — and builds a ledger of transactions you and other network members can trust.

### Advantages and disadavantages of Blockchain

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| Blockchain supports immutability, meaning it is impossible to erase or replace recorded data. Therefore, the blockchain prevents data tampering within the network. | Blockchain is considerably slower than the traditional database because blockchain technology carries out more operations |
| Blockchain is decentralized, meaning any network member can verify data recorded into the blockchain. Therefore, the public can trust the network. | Blockchain is costlier compared to a traditional database. |
| Blockchain technology is free from censorship since it does not have control of any single party. Therefore, no single authority (including governments) can interrupt the operation of the network. | Blockchain technology does not allow easy modification of data once recorded, and it requires rewriting the codes in all of the blocks, which is time-consuming and expensive |
| Blockchain creates an irreversible audit trail, allowing easy tracing of changes on the network. | Risk of property loss |
| Have a high security | Consume a lot of energy |
| Transactions widely and without intermediaries | There is a possibility that criminal organizations and individuals can do illegal transactions |

### Usecase



1. **Ethereum**

**1/ What is Ethereum**

### What is Ethereum ?

### Ethereum is a technology for building apps and organizations, holding assets, transacting and communicating without being controlled by a central authority. There is no need to hand over all your personal details to use Ethereum - you keep control of your own data and what is being shared. Ethereum has its own cryptocurrency, Ether, which is used to pay for certain activities on the Ethereum network.

### Ethereum is more like a marketplace of financial services, games, social networks and other apps that respect your privacy and cannot censor you.

### What can Ethereum do ?

### Banking for everyone: Not everyone has access to financial services. But all you need to access Ethereum and its lending, borrowing and savings products is an internet connection.

### A more private internet: You don't need to provide all your personal details to use an Ethereum app. Ethereum is building an economy based on value, not surveillance.

### A peer to peer network: Ethereum allows you to move money, or make agreements, directly with someone else. You don't need to go through intermediary companies.

### Censorship-resistant: No government or company has control over Ethereum. This decentralization makes it nearly impossible for anyone to stop you from receiving payments or using services on Ethereum.

### Commerce gurantees: Customers have a secure, built-in guarantee that funds will only change hands if you provide what was agreed. Likewise, developers can have certainty that the rules won't change on them.

### All product are composable: Since all apps are built on the same blockchain with a shared global state, they can build off each other (like legos). This allows for better products and experiences being built all the time.

### 2/Ethereum switches to Proof-of-Stakes (PoS)

### Ethereum version 1.0 and Ethereum version 2.0:

### Different between Ethereum version 1.0 and version 2.0 are consensus mechanism, beacon chain and sharding.

### Sharding:

### Any user who wants to access the Ethereum network is forced to keep records of data through the node, which stores a copy of the entire network. This means they have to download the node, compute, store and process each transaction since Ethereum exists, even if you are in the role of a user, not necessarily running the node. This is what makes everything inefficient.

### The shard chain is like any other blockchain, but the main difference is that it contains only subsets of the entire blockchain. This makes it possible for nodes to manage only a portion or a small piece of Ethereum. As a result, the transaction throughput and overall capacity of Ethereum will also increase.

### Beacon chain:

### Since shard chains work in parallel, there is now a need for something that can ensure all sharding works in sync. The beacon chain will be what covers this, by providing consensus for all shards to run in parallel.

### To be more specific, the beacon chain is a brand new blockchain that plays an important role in the formation structure of Ethereum 2.0. Conversely, without a beacon chain, information sharing between shard chains would not be possible and scalability would cease. As such, this feature is claimed to be the first to be updated on Ethereum 2.0.

### Consensus Mechanism:

### In Ethereum version 2.0, we can see it switch from using Proof of Work to Proof of Stake.

### Consensus Mechanism in Ethererum

### Define of consensus mechanism:

### Blockchains are built on top of a distributed, network of individual nodes that work together to provide on-chain information sharing. => There should be a mechanism for these nodes to synchronize to unify the information posted on the chain, this mechanism is called consensus mechanism.

### The consensus mechanism in addition to helping to ensure the core operations of blockchains also affects financial and security parameters.

### Each blockchain project will have different consensus mechanisms, in which PoW is the earliest and most widely applied consensus mechanism - currently the PoW mechanism is still applied in large networks such as ETH or BTC,...

### Proof of Work (PoW):

### What is PoW ?

### PoW is a consensus mechanism successfully developed and applied for BTC by Satoshi Nakamoto in 2009.

### Based on the characteristics of Blockchain, in PoW, miners will act as a node, using their resources to compete in solving problems - verifying transactions. With the use of their resources, miners will find possible answers, with the fastest and most correct answers will be recognized throughout the network, and the rewards will be divided among the miners. based on actual resources consumed. - For the network, solving the given problems, a new block will be added to the chain.

### Proof Of Work helps protect the network from malicious activity, ensuring that miners cannot add fake blocks to the blockchain. If a miner tries to attack the network, they will need to use more resources but they will not receive the rewards that genuine miners did.

### However, PoW also has some disadvantages such as:

### – Energy Consumption: PoW consensus, which uses a network of powerful computers to secure the network, is extremely expensive and energy-intensive. Miners need to use specialized hardware with high computing power to perform mining and receive rewards. A large amount of electricity is required to run these mining nodes continuously.

### Some also argue that these cryptographic hash calculations are useless

### because they cannot generate any business value. At the end of 2018, the Bitcoin network globally used more energy than Denmark.

### – Vulnerability: The PoW consensus is vulnerable to 51% attacks, which means that dishonest miners can theoretically gain most of the hashing power and manipulate the blockchain to their advantage.

### – Centralization: Winning a mining game requires expensive and specific hardware, usually an ASIC machine. The increased costs are unmanageable and mining is only possible for a small number of sophisticated miners. The consequence of this is the increasing centralization of the system, as it becomes a game of wealth.

### - On the other hand, it requires huge computing power and electricity to take over the PoW-based blockchain. Therefore, PoW is considered an effective way to prevent Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on the blockchain.

### 

### Proof of Stake (PoS):

### What is PoS ?

### Proof of Stake (PoS ) is a working algorithm of Blockchain. It can be understood that a user will deposit (Stake) a certain amount of assets to become a Validator (validator) of the Blockchain.

### These validators will verify transactions on the network, sending proofs into blocks. If correct, the Validators will be rewarded with tokens of the Blockchain, or transaction fees collected. If they are wrong, they will be fined to lose all or some of the deposited property.

### 

### How PoS work ?

### PoS will work by requiring participants to contribute a certain amount of coins to confirm consensus for the block. After that, the coin will be locked (locked) as collateral of the network. Upon successful confirmation (unlock), the block reward will appear and be divided among the contributors. Each participant will receive in proportion to their previous contribution

### There are 2 ways to select Validator:

### *Random selection:*

### In the "random block selection" method, validators are selected by looking for the nodes with the lowest hash value associated with the largest stake, since the size of the stake is public, it is common to other nodes can predict who will be chosen as the next validator.

### *Options based on asset holding period:*

### With this method, nodes are selected based on how long their tokens have been held as stakes. The asset holding period is calculated by multiplying the number of days the coins are held as stake by the number of coins. After a node has validated a block, their coin age is reset to zero and they have to wait a certain amount of time for another block to be verified – this prevents large asset holders from becoming dominant. blockchain value.

### 

### 

### Advantages and disadavantages of Proof of Stake:

### Overcoming the disadvantages of PoW:

### Advantages:

### + Reduce 51% attack chance - because to be able to attack the network using PoS in this way requires ownership of more than 51% of the assets on the network => Impossible.

### + Limited impact on the environment, because PoS does not require highly configurable hardware systems to solve authentication and does not need to spend too much energy to solve problems.

### Disadvantages:

### + When the user becomes a stake validator in the blockchain, the stake coins will be locked, disabled, and cannot be withdrawn by the user. So even if the coin's value increases, you can't withdraw it, and when the coin hits the bottom, you can't sell it to cover your loss, so in many cases, users will suffer losses due to the process of locking the coin. going on for too long, making it impossible for users to follow market fluctuations.

### + Besides that, there is another problem, it's about governance, for some projects, voting for a proposal is usually based on the number of tokens held, so the more tokens someone locks, the more weight they have. That's why Validator also needs users to entrust tokens to them. This leads to the case of Blockchain being centralized: A few people have too much authority, the project has to follow them, sometimes there are opinions that are not beneficial to the project but still have to be done.

### 

### 

### 3/ The Merge

### Why Ethereum need to be updated ?

### The Merge concept:

### The Merge is the next important step for Ethereum to solve the scalability issues. Simply put, it integrates two existing independent chains in the Ethereum ecosystem: the execution layer and the consensus layer (Beacon Chain).

### Progress of The Merge:

### 

### In October 2020, the staking smart contract on the PoS blockchain was deployed on the Mainnet. Users will need to stake a minimum of 32 ETH into the deposit contract to become a validator on the ETH 2.0 blockchain (blockchain using PoS, aka Beacon Chain). By the end of November 2020, the ETH 2.0 contract has reached a full stake of 16384, which is eligible for the Beacon Chain to start launching.

### On the first day of December 2020, Beacon Chain officially produced the first block.

### However, the Beacon Chain using PoS and Ethereum's Mainnet then still operated independently: the Mainnet (called the execution layer) would be responsible for transaction aggregation and validation, and the Beacon Chain (the consensus layer) would have role of controlling the consensus mechanism between validators.

### In the period from the end of 2020 until now, the Ethereum team has conducted many updates to improve the issue of gas fees on this blockchain, such as:

### – Berlin Update: Starting from block number 12,244,000, this update improves gas fees for some Ethereum tasks and supports more transaction types.

### – London Update: Launching from block number 12,965,000, an important improvement in this update is the fact that the application of

### EIP-1559 makes transaction fees more predictable for users as well as to apply a deflationary mechanism. to ETH. (EIP-1559 is an update to burn ETH coins generated by PoW - As of March 21, 2 million ETH has been

### burned with a total value of $7.2 billion).

### By October 2021, the first update for Beacon Chain – Altair (star Niu Lang) – was officially released. This update introduces some changes in the reward-punishment mechanism for validators.

### Specifically, the slashing level and the reward level for validators will both increase. In addition, this update has made it possible for users to run the node using only basic devices such as phones, without the need for a third-party infrastructure. These users are called light clients. With the help of a sync committee (a data synchronization committee, consisting of 512 validators, randomly selected by the Ethereum network and changed every 27 hours), the light clients will not need to use the process. more data to validate transactions as before; Instead, the sync committee is responsible for signing the block headers, and the light client only needs to reconfirm these signatures.

### The other two updates late 2021 (Arrow Glacier) and mid-2022 (Gray Glacier) mainly revolve around delaying the difficulty bomb until Beacon Chain is ready to merge with Ethereum's current PoW Mainnet – The Merge.

### Around June 2022, this merger took place successfully on two Ethereum testnets, Ropsten and Sepolia. By August, The Merge was stably deployed on the Goerli final testnet, bringing Ethereum's dream of realizing PoS on the Mainnet closer to the community. September 15-16 is the time when Ethereum developers estimate The Merge upgrade will take place.

### The Shanghai update for Ethereum is expected in the second half of 2023.