NATIONAL INSTITUTE OF TRANSPORT

Blockchain Technology Short Training

Introduction to Ethereum

Facilitator: Dr. Cleverence Kombe (PhD)

Introduction to Ethereum | Overview

- Ethereum wallets and clients, nodes, and miners
- Consensus Mechanisms

Ethereum Blockchain Elements | Wallets and client software

Wallets

- A wallet in Ethereum is a software application that acts as the primary interface to Ethereum, managing keys and addresses, tracking balance, and creating and signing transactions, with some wallets also able to interact with Ethereum-based decentralized applications.
- Wallets can refer to the system used to store and manage a user's keys or be part of a broader category, such as browsers.
- Balancing convenience and privacy is crucial in designing wallets, as a single private key and address is convenient but not secure, while using a new key for every transaction is best for privacy but difficult to manage.

Ethereum Blockchain Elements | Wallets and client software

Wallets

- Ethereum wallets contain keys, not ether or tokens, and there are two primary types of wallets:
- Nondeterministic wallets, where each key is independently generated from a different random number
- Deterministic wallets, where all keys are derived from a single master key
  - The seeds for deterministic wallets are often encoded as a list of words, known as the mnemonic code words, for users to write down and use in case of data-loss accidents, but it is crucial to store them safely and securely.

Ethereum Blockchain Elements | Wallets and client software

- The list of the client software and wallets that are available with Ethereum:
  - Geth - This is the official Go implementation of the Ethereum client.
  - Eth - This is the C++ implementation of the Ethereum client.
  - Parity - This implementation is built using Rust and developed by Parity technologies.
  - Trinity - Trinity is the implementation of the Ethereum protocol. It is written in Python.

Ethereum Blockchain Elements | Wallets and client software

Geth

- Geth is the official Go implementation of the Ethereum client, and it is written in the Go programming language. This implementation is responsible for syncing the Ethereum blockchain, creating and submitting transactions, and mining blocks.
- It provides a command-line interface (CLI) that enables users to interact with the Ethereum network through their terminals.
- Geth can also function as a node in the Ethereum network, allowing it to communicate with other nodes, propagate transactions, and synchronize blockchain data. It is widely considered to be one of the most stable and reliable implementations of the Ethereum client.

Ethereum Blockchain Elements | Wallets and client software

Eth

- Eth is a C++ implementation of the Ethereum client. It provides similar functionality to Geth, including syncing the blockchain, creating and submitting transactions, and mining blocks.
- Eth is also equipped with a CLI interface that allows users to interact with the Ethereum network through their terminals..
- Eth is popular among developers who prefer to work with the C++ programming language. It is also used by some Ethereum wallets and dApps, although it is less widely adopted than Geth.

Ethereum Blockchain Elements | Wallets and client software

Parity

- Parity is an implementation of the Ethereum client that is built using the Rust programming language.
- Parity is designed to be highly performant and secure, and it includes several advanced features that are not present in other Ethereum clients.
- For example, Parity supports sharding, which enables the Ethereum network to scale more efficiently by dividing the workload among multiple nodes.
- Parity also includes a graphical user interface (GUI) that makes it easier for non-technical users to interact with the Ethereum network. .

Ethereum Blockchain Elements | Wallets and client software

Trinity

- Trinity is an implementation of the Ethereum protocol that is written in Python. It provides similar functionality to other Ethereum clients, including syncing the blockchain, creating and submitting transactions, and mining blocks.
- Trinity is designed to be modular and extensible, which makes it easy for developers to customize the client to suit their needs.
- Trinity is also used by some Ethereum wallets and dApps, although it is less widely adopted than Geth and Parity. Despite its relative lack of adoption, Trinity is considered to be a stable and reliable Ethereum client that provides a useful alternative to other implementations.

Ethereum Blockchain Elements | Wallets and client software

Light clients

- Simple Payment Verification (SPV) clients download only a small subset of the blockchain. This allows low resource devices, such as mobile phones, embedded devices, or tablets, to be able to verify the transactions.
- A complete Ethereum blockchain and node are not required in this case, and SPV clients can still validate the execution of transactions. SPV clients are also called light clients.
- The critical difference between clients and wallets is that clients are full implementations of the Ethereum protocol, which support mining, account management, and wallet functions.
- In contrast, wallets only store the public and private keys, provide essential account management, and interact with the blockchain for usually only payment (transfer of funds) purposes.

Ethereum Blockchain Elements | Wallets and client software

Light clients

- In Ethereum, there are several SPV clients available, including:
  - MetaMask: MetaMask is a browser extension that allows users to interact with the Ethereum network using a simple user interface. It functions as an SPV client, allowing users to view account balances and interact with decentralized applications without downloading the entire blockchain.
  - MyEtherWallet (MEW): MEW is a web-based Ethereum wallet that also functions as an SPV client. Users can create and manage Ethereum accounts, view account balances, and send and receive ETH and other tokens without downloading the entire blockchain.

Ethereum Blockchain Elements | Wallets and client software

Light clients

- In Ethereum, there are several SPV clients available, including:
  - Trust Wallet: Trust Wallet is a mobile wallet that allows users to store and manage Ethereum and other cryptocurrencies. It also functions as an SPV client, allowing users to view account balances and send and receive transactions without downloading the entire blockchain.
  - Infura: Infura is a web3 provider that offers a free API service for Ethereum developers. It allows developers to interact with the Ethereum network using an SPV client, without the need to download and manage the entire blockchain.

Ethereum Blockchain Elements | Nodes and miners

- Miners perform the most important operation of the Ethereum blockchain, called mining.
- The Ethereum network contains different nodes. Some nodes act only as wallets, some are light clients, and a few are full clients running the full blockchain. One of the most important types of nodes are mining nodes.
- As a result of the mining operation, currency (ether) is awarded to the nodes that perform mining operations. These mining nodes are known as miners.
- Miners are paid in ether as an incentive for them to validate and verify blocks made up of transactions. The mining process helps secure the network by verifying computations.

Ethereum Blockchain Elements | Nodes and miners

- At a theoretical level, a miner node performs the following functions:
  - It listens for the transactions broadcasted on the Ethereum network and determines the transactions to be processed.
  - It determines stale ommer blocks and includes them in the blockchain.
  - It updates the account balance with the reward earned from successfully mining the block.
  - Finally, a valid state is computed, and the block is finalized, which defines the result of all state transitions.

Ethereum Blockchain Elements | Nodes and miners

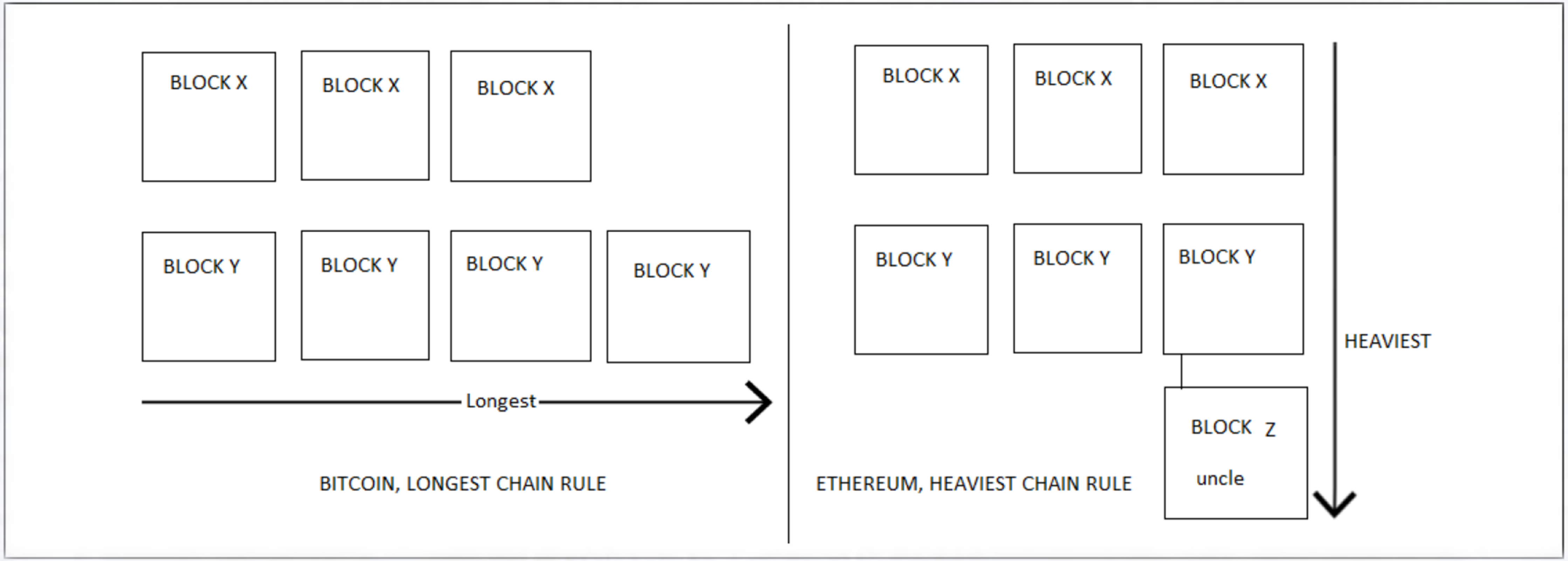
- The current method of mining is based on PoW, which is similar to that of Bitcoin.
- When a block is deemed valid, it has to satisfy not only the general consistency requirements, but it must also contain the PoW for a given difficulty.
- The PoW algorithm is due to be replaced by the PoS algorithm with the release of Serenity.
- An algorithm named Casper has been developed that will replace the existing PoW algorithm in Ethereum.
- This is a security deposit based on the economic protocol where nodes are required to place a security deposit before they can produce blocks. Nodes have been named bonded validators in Casper, whereas the act of placing the security deposit is named bonding.

Ethereum Blockchain Elements | The consensus mechanism

- The consensus mechanism in Ethereum is based on the Greedy Heaviest Observed Subtree (GHOST) protocol proposed initially by Zohar and Sompolinsky in December 2013.
- Ethereum uses a simpler version of this protocol, where the chain that has the most computational effort spent on it to build it is identified as the definite version.
- Another way of looking at it is to find the longest chain, as the longest chain must have been built by consuming adequate mining efforts.
- The GHOST protocol was first introduced as a mechanism to alleviate the issues arising out of fast block generation times that led to stale or orphaned blocks.
- In GHOST, stale blocks, or ommers, are added in calculations to figure out the longest and heaviest chain of blocks.

Ethereum Blockchain Elements | The consensus mechanism

- The following diagram shows a quick comparison between the longest and heaviest chains:



BITCOIN, LONGEST CHAIN RULE

ETHEREUM, HEAVIEST CHAIN RULE

Ethereum Blockchain Elements | The consensus mechanism

- The preceding diagram shows two rules of figuring out which blockchain is the canonical version of truth.

- In the case of Bitcoin, shown on the left-hand side in the diagram, the longest chain rule is applied, which means that the active chain (true chain) is the one that has the most amount of PoW done.

- In the case of Ethereum, the concept is similar from the point of view of the longest chain, but it also includes ommers, the orphaned blocks, which means that it also rewards those blocks that were competing with other blocks during mining to be selected and performed significant PoW, or were mined exactly at the same time as others but did not make it to the main chain.

- This makes the chain the heaviest instead of the longest because it also contains the orphaned blocks. This is shown on the right-hand side of the diagram.

Ethereum Blockchain Elements | The consensus mechanism

Forks in the blockchain

- As the blockchain progresses (more blocks are added to the blockchain) governed by the consensus mechanism, on occasion, the blockchain can split into two. This phenomenon is called forking.

- A fork can be intentional or non-intentional. Usually, as a result of a major protocol upgrade, a hard fork is created, while an unintentional fork can be created due to bugs in the software.

- This temporary fork occurs when a block is created almost at the same time and the chain splits into two, until it finds the longest or heaviest chain to achieve eventual consistency

Ethereum Blockchain Elements | The consensus mechanism

Ethash

- To facilitate consensus, a PoW algorithm is used. In Ethereum, the algorithm used for this purpose is called **Ethash**.
- Ethash is the name of the PoW algorithm used in Ethereum.
- Originally, this was proposed as the Dagger-Hashimoto algorithm, but much has changed since the first implementation, and the PoW algorithm has now evolved into what's known as Ethash.
- Similar to Bitcoin, the core idea behind mining is to find a nonce (a random arbitrary number), which, once concatenated with the block header and hashed, results in a number that is lower than the current network difficulty level.

Ethereum Blockchain Elements | The consensus mechanism

Ethash

- Initially, the difficulty was low when Ethereum was new, and even CPU and single GPU mining was profitable to a certain extent, but that is no longer the case.
- Now, only either pooled mining or large GPU mining farms are used for profitable mining purposes.
- Ethash is a memory-hard algorithm, which makes it difficult to be implemented on specialized hardware.
- As in Bitcoin, ASICs have been developed, which have resulted in mining centralization over the years, but memory-hard PoW algorithms are one way of thwarting this threat, and Ethereum implements Ethash to discourage ASIC development for mining.

Ethereum Blockchain Elements | The consensus mechanism

Ethash

- Ethash is a memory-hard algorithm and developing ASICs with large and fast memories is not feasible. This algorithm requires subsets of a fixed resource called Directed Acyclic Graph (DAG) to be chosen, depending on the nonce and block headers.
- DAG is a large, pseudo-randomly generated dataset. This graph is represented as a matrix in the DAG file created during the Ethereum mining process. The Ethash algorithm expects the DAG as a two-dimensional array of 32-bit unsigned integers.
- Mining can only start when DAG is completely generated the first time a mining node starts. This DAG is used as a seed by the algorithm called Ethash. According to current specifications, the epoch time is defined as 30,000 blocks, or roughly 6 days.

Ethereum Blockchain Elements | The consensus mechanism

Ethash

- The Ethash algorithm requires a DAG file to work.
- A DAG file is generated every epoch, which is 30,000 blocks.
- DAG grows linearly as the chain size grows.
- Currently, the DAG size is around 3.5 GB (as of block 9325164) and epoch number 310.
- The Ethash protocol works as follows:

  1. First, the header from the previous block and a 32-bit random nonce is combined using Keccak-256.

Ethereum Blockchain Elements | The consensus mechanism

Ethash

- The Ethash protocol works as follows:

2. This produces a 128-bit structure called mix.
3. mix determines which data is to be picked up from the DAG.
4. Once the data is fetched from the DAG, it is "mixed" with the mix to produce the next mix, which is then again used to fetch data from the DAG and subsequently mixed. This process is repeated 64 times.
5. Eventually, the 64th mix is run through a digest function to produce a 32-byte sequence.
6. This sequence is compared with the difficulty target. If it is less than the difficulty target, the nonce is valid, and the PoW is solved. As a result, the block is mined. If not, then the algorithm repeats with a new nonce.

Ethereum Blockchain Elements | The consensus mechanism

Ethash

- The current reward scheme is 2 ETH for successfully finding a valid nonce. In addition to receiving 2 ether, the successful miner also receives the cost of the gas consumed within the block and an additional reward for including stale blocks (uncles) in the block.

- A maximum of two ommers are allowed per block and are rewarded with 7/8 of the normal block reward.

- In order to achieve a 12-second block time, block difficulty is adjusted at every block. The rewards are proportional to the miner's hash rate, which means how fast a miner can hash.

- In order to achieve a 12-second block time, block difficulty is adjusted at every block. The rewards are proportional to the miner's hash rate, which means how fast a miner can hash.

Ethereum Blockchain Elements | The consensus mechanism

Ethash

- The current reward scheme is 2 ETH for successfully finding a valid nonce. In addition to receiving 2 ether, the successful miner also receives the cost of the gas consumed within the block and an additional reward for including stale blocks (uncles) in the block.
- A maximum of two ommers are allowed per block and are rewarded with 7/8 of the normal block reward.
- In order to achieve a 12-second block time, block difficulty is adjusted at every block. The rewards are proportional to the miner's hash rate, which means how fast a miner can hash.

Ethereum Blockchain Elements | The consensus mechanism

Ethash

- You can use an ether mining calculator to calculate what hash rate is required to generate profit.
  - One example of such a calculator is https://etherscan.io/ethermining-calculator.
- Mining can be performed by simply joining the Ethereum network and running an appropriate client.
- The key requirement is that the node should be fully synched with the main network before mining can start.

Ethereum Blockchain Elements | The consensus mechanism

Ethash

- You can use an ether mining calculator to calculate what hash rate is required to generate profit.
- Mining can be performed by simply joining the Ethereum network and running an appropriate client.
- The key requirement is that the node should be fully synched with the main network before mining can start.

Ethereum Blockchain Elements | The consensus mechanism

Casper

- Casper is a proposed consensus algorithm for Ethereum that would replace the current Proof of Work (PoW) algorithm with Proof of Stake (PoS). The goal of Casper is to increase the scalability and security of the Ethereum network by reducing energy consumption and enabling faster transaction processing.

- Casper is not a single algorithm but rather a family of PoS algorithms that are being developed by the Ethereum community. The first version of Casper was called "Casper the Friendly Finality Gadget" and was introduced in 2015 by Ethereum co-founder Vitalik Buterin.

- Casper has undergone several revisions since then, and the latest version is called Casper FFG (Friendly Finality Gadget).

Ethereum Blockchain Elements | The consensus mechanism

Casper

- In Casper FFG, validators are required to lock up a certain amount of Ethereum (ETH) as collateral to participate in the consensus process. Validators are randomly selected to create new blocks, and their probability of being selected is proportional to the amount of ETH they have staked.

- Validators are also required to attest to the validity of other blocks, and they can be penalized for attesting to conflicting blocks or attempting to double-spend.

- Casper FFG introduces a new concept called "finality" to the Ethereum network. Finality means that once a block has been added to the blockchain, it is guaranteed to be a part of the canonical chain forever.

Ethereum Blockchain Elements | The consensus mechanism

Casper

- Finality differ from PoW, where there is a possibility that a competing chain with more computational power could eventually overtake the main chain, resulting in a reorganization of the blockchain.
- One of the benefits of Casper FFG over PoW is that it is more energy-efficient, as it does not require validators to perform computationally intensive calculations.
- Casper FFG is also designed to be more secure, as it incentivizes validators to act honestly and penalizes them for acting maliciously.

Introduction to Blockchain | Summary

► **In this topic, we discussed:**

- Wallets and client software
- Nodes and miners
- The consensus mechanism.

THANK YOU