SMU FinTech Publication

Research – The Evolution of Ethereum

Tuesday, 30 June 2020
By: Nah Hui Xian

The Evolution of Ethereum

Introduction to Ethereum's unique protocols and how it has evolved over the years

Introduction to Ethereum

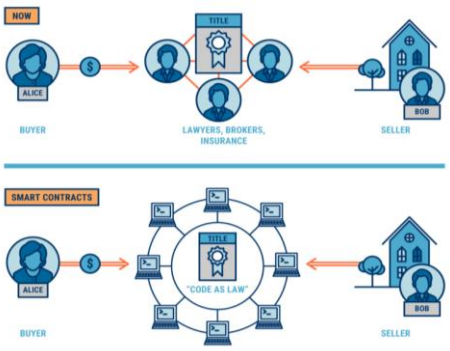
Ethereum was created with the vision of becoming a world computer that would decentralize and democratize the existing client-server model that the internet functions within. To understand this vision, we have to first understand the centralized design of the internet.

Our personal data and passwords are largely stored in clouds and servers owned by technology giants including Amazon, Facebook and Google. There is almost no activity on the web that happens without some sort of intermediary or third party. While this set up brings upon conveniences such as teams of tech specialists deployed to store and secure this data, as well as removed costs that come with hosting and uptime, there remains a vulnerability: A hacker can gain unwelcome access to user's files without that user's knowledge by influencing or attacking a third party service. This flaw of the internet has motivated a splintered movement around using new tools such as blockchain technology to decentralize the internet. Ethereum is one of the technologies involved in this movement – with a goal to utilize blockchain to replace internet third parties that store, transfer data, and keep track of complex financial instruments.

How Ethereum Functions

The Ethereum network is a DIY platform for decentralized applications (DAPPS), with thousands of independent computers running it. Once a program is deployed to the Ethereum network, these independent computers (also known as nodes) will execute the program as it is written. Hence, this concept allows servers and clouds to be replaced by the thousands of nodes run by volunteers across the globe. Its coding language Solidity is used to write smart contracts that represents the logic that runs the DAPPS. Ethereum developers will indicate the terms in which their DAPP functions, and the Ethereum network will execute it.

These sets of terms and the resulting executed actions are called smart contracts: that deals with all aspects of the contract including enforcement, management, performance, and payment. Once a smart contract is deployed on the Ethereum network, it cannot be edited or corrected, even by its original owner. Consequentially, when complex contracts are created in the Ethereum network, difficulties arise in handling such contracts with perfect accuracy every possible way in which the contract can be executed. This difficulty is illustrated in the DAO event – one of the prominent events that shaped the evolution of Ethereum to become what it is today.



The use of smart contracts replaces the need for intermediaries (lawyers, insurance, etc.), decentralizing transactions.

Ethereum as a Currency

Ethereum is a collection of computers working together as one super computer to execute the code that powers DAPPS – given that it costs money to get the machines, power them up, store them and cool them if needed, ether (the price of Ethereum) was invented to incentivize people to run the Ethereum protocol on their computer. This is similar to the way bitcoin miners get paid for maintaining the bitcoin blockchain. In order to deploy a smart contract to the Ethereum platform, it's author must pay to do so. This payment is done in the form of ether.

Ethereum's first initial coin offering (ICO) occurred in 2014. During it's ICO, it cost around $0.40 to buy one ether. Today, one ether is valued at $210.40![2] (9th May 2020) The price of ether has increased immensely after the growth of the Ethereum network through the ICO hype that started in 2017. Ether can be purchased via finding someone online or in-person who has ether and wants to trade. It is also possible to buy ether with another currency – as bitcoin is the most commonly used cryptocurrency, people around the world are more likely to want to trade Ether for Bitcoin.

Receiving and Spending Ether

The two main components that users require for identification is the public key and the private key. Usually represented as a scrambled string of numbers and letters, the two keys are linked together by cryptography. The public key represents an address for where money can be sent to and hence can be sent to others. The private key is used to sign funds over and hence spend ether. The benefit of this system is that users can generate an identification number for their funds at any time and need not wait for a bank to approve their application.

Ethereum Wallets

Ether – the unique pieces of code that represents both the price of Ethereum and allows for updates to the blockchain's ledger is stored in Ethereum wallets. Ethereum wallets comprise desktop wallets, mobile wallets, hardware wallets and paper wallets.

Choosing a particular wallet depends on an individual's preferences for convenience and security, with these two concepts often at odds with one another. [1]

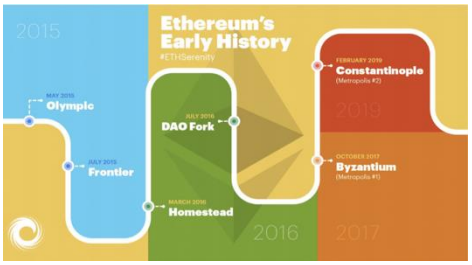
1. Desktop wallets: run on computers, requires the user to download an Ethereum client. This will take a few days, and the wallet must stay in sync with the latest transactions on blockchain.

2. Mobile wallets: can be downloaded on a smartphone because they require less data to be downloaded to connect to the network and make transactions. While it provides a great deal of convenience to the user, it compromises on security. Full Ethereum clients validate transactions themselves and hence offers a more secure way of receiving transactions.

3. Hardware wallets: Offers the best of both worlds in terms of security and convenience by allowing secure devices to be detached from the internet and transactions to be signed without being online.

4. Paper wallets: Cold storage option wherein a user prints a private key on a slip of paper and locks it somewhere secure like a deposit box. The best practice for this option is to create multiple copies of the private key and stash them in different secure locations, in case one is lost or destroyed.

Evolution of Ethereum



An illustration of Ethereum's History

In 2013, Vitalik Buterin[3] - Ethereum's co-founder - released a whitepaper where he described Ethereum as a blockchain based decentralizing mining network and software development platform rolled into one. This begin the first stage of Ethereum's development.

Pre-launch: Olympic

Before the Ethereum blockchain sprung into public existence in July 2014, the blockchain underwent the Olympic – it's ninth and final proof of concept open testnet, with the main purpose to stress-test the network. Vitalik announced a total reward of 25,000 ether to developers who stress-tested the network. The intention of this stress-test was to provide insight into how the protocol would handle high traffic.

Stage one: Frontier

After months of stress-testing, the Ethereum network was released in its official public main net launch in July 20, 2015. Its genesis block was mined into existence and its community begin to grow.

The Frontier protocol contained a series of crucial characteristics:

1. Block Reward: Miners who successfully mine a block into existence on the Ethereum blockchain are reward in terms of 5 ether per block.

2. Gas: To provide a buffer time for miners to start their operations on Ethereum and early adopters to install their clients, the gas limit per block was set at 5000 gas in the first few days after the launch of the blockchain.

3. Canary Contracts: Canary contracts were included to notify users that a particular chain was bad or vulnerable. Contracts that had an issue were given a 0 and clients were notified so they would not mine off that broken chain, and contracts that had a 1 were safe to mine. Canary contracts were a heavily centralized but necessary protection mechanism early in Ethereum's existence.

4. Usability: The original design of the Ethereum platform catered only to developers and it only featured command-line interfaces.

After some initial errors were fixed and the platform was adapted for end users, Ethereum launched 'Homestead' – its first public version, entering it's second stage

Stage two: Homestead

The Homestead upgrade was executed on the network on May 14, 2016. This upgrade included three major improvements: Removed canary contracts, introduced new code into Solidity and introduced the Mist wallet. The Mist wallet could be used to both store ether and write smart contracts. The Homestead upgrade was one of the earliest implementations of Ethereum Improvement Proposals (EIPs). EIPs are proposals put forward by the Ethereum community to be included in network upgrades.

The DAO Event

DAO refers to decentralized autonomous organization – where users were allowed to deposit money into the DAO and get returns based on the money that the DAO made. The decisions made by the DAO would be crowdsourced and hence decentralized. This project attracted many of Ethereum's earliest investors, and by May 2016, 14% of Ethereum's tokens invested into the DAO. The project went live at the end of May 2016 and by June 2016, it became the subject of an attack where someone managed to drain the DAO out of money – approximately 3.6 million ether were effectively stolen![4] In the aftermath of this incident, the members of the DAO and the Ethereum community engaged in debate about what to do next. To retrieve back all the stolen ether, a hard fork (radical change to the protocol of a blockchain network that makes the previous transactions invalid) would be needed.

As many believed that the attack was akin to a lawyer exploiting a legal loophole to get his client out of charges and hence a valid maneuver that did not technically break any rules, the decision of a hard fork did not reach a consensus. Hence, Ethereum diverged into two different versions. The users who disagreed with the hard fork continued to support the old version of Ethereum - Ethereum Classic.

Stage 3: Metropolis

The next stage of Ethereum's evolution is Metropolis. Metropolis was implemented in two stages – Byzantium and Constantinople. The main goal of the metropolis stage was to transition the network from the Proof-of-Work method to the Proof-of-State method of consensus. The Proof-of-Work method leverages mining wherein nodes solve complex equations to receive cryptocurrency and block ownership. This method has been criticized as making the rich richer as chances of solving the complex equations are greatly improved in the Proof-of-Work method based on the computation power a person can afford, incentivizing major organizations to set up mining pools and placing individual miners at a competitive disadvantage.

The Proof-of-State method encompasses a method called 'foraging' – a random selection where a node's chances of receiving the next block increases with the proportion of assets staked in the mining.

Byzantium Fork

The Byzantium upgrade went live in October 2017 and introduced nine EIPs to the system. This update disincentivized mining by reducing the reward for mining a block from 5 ether to 3 ether to aid the transition into the Proof-of-State method. It also made the blockchain more compatible with cryptographic primitives to enhance the privacy system and introduce a more autonomous flow of assets within the system. Cryptographic primitives refer to a function that provides cryptographic evidence of a transaction's completion while keeping all participating parties anonymous.

Constantinople Fork

The Constantinople upgrade went live on Feb 28, 2019. The Constantinople upgrade is made up of 2 stages: Petersburg and Istanbul.

Petersburg was centered around increasing the difficulty of mining and introduced a total of five EIPs. One of the five EIPs - EIP 1234 – was a hard fork which further reduced block rewards from 3 ether to 2 ether, further deterring miners by reducing profits.

Istanbul referred to a system-wide upgrade that changed Ethereum's mining protocol and code execution. It activated six EIPs including the introduction of the ProgPoW – a proof of work algorithm designed to close the efficiency gap available to specialized application-specific integrated circuit miners.

Muir Glacier Fork

The Muir Glacier update was activated on Jan 2, 2020 with the improvement proposal EIP 2384. EIP 2384 aims to delay the difficulty bomb, a built-in algorithm of the Ethereum blockchain that could drastically increase the difficulty in mining a new block if left accounted for. This update is designed to delay the difficulty bomb for another 611 days.

Stage 4: Serenity

This stage represents the ultimate goal of the Ethereum Blockchain. It will mark a complete transition to the PoS model. To reach this stage, Ethereum is attempting to transfer its entire economy onto a new network - Ethereum 2.0

Ethereum 2.0

Ethereum 2.0 is set to launch as early as July 2020. The network will allow scalability by via sharding – database partitioning that separates very large databases into smaller and faster parts called data shards. In the initial stages, Ethereum 2.0 is likely to only operate as a test network for the new proof of stake consensus system.

Most economic activity and smart contracts will remain on the original Ethereum network which will continue to exist as a parallel system to Ethereum 2.0. Eth1 will continue as a proof of work chain and Eth2 will operate under the new proof of stake system.

Eth1 can be converted into Eth2, but the reverse is not possible. This means that Eth2 should trade at a price less than or equal to the price of Eth1. However, in the initial stages of the transition, it is unlikely that Eth2 will even have a price or be supported by exchanges as the coin can only be used for staking and not be used for basic transactions.

Evaluation of the Ethereum Network

Ethereum's promise to the world was to create a decentralized world computer that would allow developers to upload applications to the blockchain for use by anyone, anywhere in the world. Five years after its launch in 2015, no single application on the Ethereum network has been able attract mainstream adoption. The daily active users of its top applications still pale in comparison to those of Facebook and Google. Only with solving the key problems around scalability and performance will Ethereum be able to achieve its vision of reaching billions of people around the world with their decentralized applications. It is our hope that Ethereum 2.0 will be able to achieve this mission in the years to come.

Contact: Jax Khor Jia Xuan, Research Director
jxkhor.2018@business.smu.edu.sg

Sources:

1. Ethereum 101: Who Created Ethereum? (n.d.). Retrieved from https://www.coindesk.com/learn/ethereum-101/who-created-ethereum
2. Ethereum Price Index – Real-time Ethereum (ETH) Price Charts. (2019, March 6). Retrieved from https://www.coindesk.com/price/Ethereum Liebkind, J. (2020, March 2020). How Blockchain Technology is Changing Real Estate. Retrieved from Investopedia: https://www.investopedia.com/news/how-blockchain-technology-changing-real-estate/
3. Marr, B. (2018, March 20). Blockchain: A Very Short History Of Ethereum Everyone Should Read. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/02/02/blockchain-a-very-short-history-of-ethereum-everyone-should-read/#15f306c31e89
4. Ethereum-The Whole Forking History. (2020, January 10). Retrieved from https://blockchain.news/news/ethereum-the-whole-forking-history