ETHEREUM'S HISTORY: FROM ZERO TO 2.0

Jianing Wu – Senior Analyst, Research
07/15/2021

Vitalik Buterin came up with the idea of Ethereum in 2013 at the age of 19. Later that year, he published a white paper describing Ethereum as "a next-generation smart contract and decentralized application platform,"[1] marking the beginning of Ethereum's journey.

Ethereum is now the second-largest cryptocurrency by market capitalization, accounting for approximately 18% of the cryptocurrency market. Its success cannot be separated from a creatively elegant idea, a nicely executed development process and the continued support of the community.

In this article, we will look back at the history of Ethereum's development and provide an outlook for what's upcoming.

Pre-launch

Ethereum's invention was inspired by Bitcoin.

Bitcoin established the foundation for decentralized blockchain technology. But its functionality is limited to peer-to-peer electronic cash transfers. Seeing this limitation, Buterin wanted to expand blockchain's functionality to programmable apps.

At first, he wanted to achieve this by adding a more advanced scripting language on top of Bitcoin to allow smart contracts processing, but this idea was rejected by the Bitcoin community. Then, Buterin decided to create a completely new blockchain to enable this "world computer."

In late 2013, Buterin published his white paper outlining the idea of Ethereum. In January 2014, Ethereum was first announced at The North American Bitcoin Conference in Miami. The idea attracted many developers, including Gavin Wood, who published the famous "Yellow Paper" on the technical implementation for Ethereum[2].

By the end of 2014, Ethereum had its first crowdfunding, raising more than $18 million by selling the native token, ether. Early Ethereum founders and developers[2] also hosted the first Ethereum conference, called DEVCON0, during which the developers met for the first time.

Execution

Ethereum's development was planned with four main stages. Each stage represents a necessary system-wide upgrade of the network, at which point old versions are no longer supported. They are also called "hard forks."

Within the main stages, there have been planned and unplanned sub-upgrades.

July 30, 2015–March 14, 2016: Implementing basic technical foundation ("Frontier" phase)

On July 30, 2015, the first version of Ethereum (Ethereum 1.0) was released, called Frontier. It had the two most basic functions: to enable users to mine ether and run smart contracts. The purpose of the initial stage was to get the network started, so miners could set up their mining processes and developers could test their decentralized applications (DApps).

A minor fork called **Frontier Thawing** followed, during which gas was limited to 5,000 per transaction, to ensure transaction fees were not too high and hindering usage.

March 14, 2016–October 16, 2017: Improving infrastructure to address security issues ("Homestead" phase)

If Frontier was the working version of Ethereum, **Homestead** was the "safer" version of Frontier.

Ethereum's security vulnerability was brought to public attention with the DAO hack. Launched in 2016, DAO was an innovative idea to allow users to crowd source funds. However, it failed due to a bug in its smart contract code that hackers exploited to steal a portion of the organization's funds. This event resulted in a controversial decision to implement a hard fork on the Ethereum network to return the stolen funds. Part of the community did not accept the change, creating a branch called Ethereum Classic, which still exists today.

After suffering several DoS (denial-of-service) attacks, two sub-upgrades called **Tangerine Whistle** and **Spurious Dragon** were released to address security issues, through adjusting gas fees and implementing state clearing.

October 16, 2017–January 2, 2020: Solving challenges that come with expansion and growth ("Metropolis" phase)

Metropolis was a comprehensive improvement of Ethereum's security, privacy and scalability. It solved many challenges Ethereum faced during its scaling process and brought a lighter, more efficient experience for developers and users. Because the update was so complicated, it was released in two steps: **Byzantium** and **Constantinople**.

Byzantium was the first stage, with main upgrades introduced in nine patches, also called Ethereum improvement protocols (EIP). These included important features such as zk-SNARKs[3], account abstraction[4] and the difficulty bomb[5].

Constantinople was supposed to launch in mid-2018 but was delayed for more than half a year due to a critical bug found hours before its intended launch. Constantinople was meant to fix any problems that might arise from Byzantium's implementation. In addition, it laid the groundwork for the transition from proof-of-work to proof-of-stake, which will significantly reduce Ethereum's validation energy consumption.

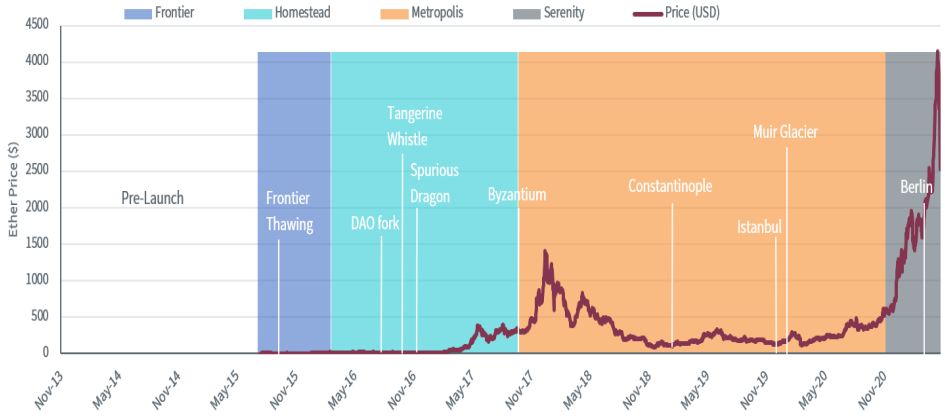
January 2, 2020–2022: Ethereum 2.0 to be more scalable, secure and sustainable ("Serenity" phase)

Currently, the Serenity stage is still in development. Also known as Ethereum 2.0, this version aims to advance Ethereum to a level that can be broadly used without encountering security or high-volume issues.

Specifically, it intends to solve two main challenges Ethereum is facing: a clogged network that can only handle a limited number of transactions per second (with increased gas fees for faster transactions), and the large consumption of energy that comes with the proof-of-work mechanism.[6]

Two of the major upgrades are the shift from proof-of-work to proof-of-stake and the implementation of shard chains which will spread the workload of the network.[7] Ethereum 2.0 is envisioned to be more scalable, secure and sustainable, although when (or if) it will ultimately be implemented, and other fallout issues, remain unclear.

Ether Price And Development Stages



Source: WisdomTree, Bloomberg, as of 5/20/2021. November 2013 - May 2021. **Historical performance is not an indication of future performance and any investments may go down in value. Istanbul, Muir Glacier, and Berlin are three sub-hard forks in Ethereum's development stages.**

Conclusion

After eight years of development, Ethereum has gone from an idea to a vivid ecosystem, supported by one of the largest developer communities in the crypto space. As a software platform, it needs to evolve to address its issues. Its community is progressive and has implemented several significant changes over time. Some of the most important changes still lie ahead, and we will address them in more detail in future posts.

[1] https://ethereum.org/en/whitepaper/

[2] Early founders included Vitalik Buterin, Anthony Di Iorio, Charles Hoskinson, Mihai Alisie, Amir Chetrit, Joseph Lubin, Gavin Wood and Jeffrey Wilcke.

[3] "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge," and refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier.

[4] https://eips.ethereum.org/EIPS/eip-2938

[5] Refers to the increase of difficulty in Ethereum's proof-of-work consensus mechanism.

[6] Proof-of-work is a consensus mechanism used to verify blockchain transactions' validity, through solving computationally intensive puzzles using miners' computers' processing power.

[7] Proof-of-stake is another consensus mechanism that is used to verify blockchain transactions. However, it does so by using miners' existing coins as a stake in the validation process, which demands less computer processing power.

money laundering) procedures, non-compliance with applicable rules and regulations, technical glitches, hackers, malware or other reasons, which could negatively impact the price of any cryptocurrency traded on such exchanges or reliant on a settlement facility or otherwise may prevent access or use of the crypto asset. Crypto assets can experience unique events, such as forks or airdrops, which can impact the value and functionality of the crypto asset. Crypto asset transactions are generally irreversible, which means that a crypto asset may be unrecoverable in instances where: (i) it is sent to an incorrect address, (ii) the incorrect amount is sent, or (iii) transactions are made fraudulently from an account. A crypto asset may decline in popularity, acceptance or use, thereby impairing its price, and the price of a crypto asset may also be impacted by the transactions of a small number of holders of such crypto asset. Crypto assets may be difficult to value and valuations, even for the same crypto asset, may differ significantly by pricing source or otherwise be suspect due to market fragmentation, illiquidity, volatility and the potential for manipulation. Crypto assets generally rely on blockchain technology and blockchain technology is a relatively new and untested technology which operates as a distributed ledger. Blockchain systems could be subject to Internet connectivity disruptions, consensus failures or cybersecurity attacks, and the date or time that you initiate a transaction may be different than when it is recorded on the blockchain. Access to a given blockchain requires an individualized key, which, if compromised, could result in loss due to theft, destruction or inaccessibility. In addition, different crypto assets exhibit different characteristics, use cases and risk profiles. Information provided by WisdomTree regarding digital assets, crypto assets or blockchain networks should not be considered or relied upon as investment or other advice, as a recommendation from WisdomTree, including regarding the use or suitability of any particular digital asset, crypto asset, blockchain network or any particular strategy. WisdomTree is not acting and has not agreed to act in an investment advisory, fiduciary or quasi-fiduciary capacity to any advisor, end client or investor, and has no responsibility in connection therewith, with respect to any digital assets, crypto assets or blockchain networks.

For standardized performance and the most recent month-end performance click here NOTE, this material is intended for electronic use only. Individuals who intend to print and physically deliver to an investor must print the monthly performance report to accompany this blog.

View the online version of this article here.

IMPORTANT INFORMATION

U.S. investors only: Click here to obtain a WisdomTree ETF prospectus which contains investment objectives, risks, charges, expenses, and other information; read and consider carefully before investing.

There are risks involved with investing, including possible loss of principal. Foreign investing involves currency, political and economic risk. Funds focusing on a single country, sector and/or funds that emphasize investments in smaller companies may experience greater price volatility. Investments in emerging markets, currency, fixed income and alternative investments include additional risks. Please see prospectus for discussion of risks.

Past performance is not indicative of future results. This material contains the opinions of the author, which are subject to change, and should not to be considered or interpreted as a recommendation to participate in any particular trading strategy, or deemed to be an offer or sale of any investment product and it should not be relied on as such. There is no guarantee that any strategies discussed will work under all market conditions. This material represents an assessment of the market environment at a specific time and is not intended to be a forecast of future events or a guarantee of future results. This material should not be relied upon as research or investment advice regarding any security in particular. The user of this information assumes the entire risk of any use made of the information provided herein. Neither WisdomTree nor its affiliates, nor Foreside Fund Services, LLC, or its affiliates provide tax or legal advice. Investors seeking tax or legal advice should consult their tax or legal advisor. Unless expressly stated otherwise the opinions, interpretations or findings expressed herein do not necessarily represent the views of WisdomTree or any of its affiliates.

The MSCI information may only be used for your internal use, may not be reproduced or re-disseminated in any form and may not be used as a basis for or component of any financial instruments or products or indexes. None of the MSCI information is intended to constitute investment advice or a recommendation to make (or refrain from making) any kind of investment decision and may not be relied on as such. Historical data and analysis should not be taken as an indication or guarantee of any future performance analysis, forecast or prediction. The MSCI information is provided on an "as is" basis and the user of this information assumes the entire risk of any use made of this information. MSCI, each of its affiliates and each entity involved in compiling, computing or creating any MSCI information (collectively, the "MSCI Parties") expressly disclaims all warranties. With respect to this information, in no event shall any MSCI Party have any liability for any direct, indirect, special, incidental, punitive, consequential (including loss profits) or any other damages (www.msci.com)

Jonathan Steinberg, Jeremy Schwartz, Rick Harper, Christopher Gannatti, Bradley Krom, Tripp Zimmerman, Michael Barrer, Anita Rausch, Kevin Flanagan, Brendan Loftus, Joseph Tenaglia, Jeff Weniger, Matt Wagner, Alejandro Saltiel, Ryan Krystopowicz, Jianing Wu, and Brian Manby are registered representatives of Foreside Fund Services, LLC.

WisdomTree Funds are distributed by Foreside Fund Services, LLC, in the U.S. only.

You cannot invest directly in an index.

DEFINITIONS

Cryptocurrency : a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend.

Bitcoin (the currency) : A digital currency (also called a cryptocurrency) created in 2009, which is operated by a decentralized authority as opposed to a traditional central bank or monetary authority.

Blockchain : a distributed ledger system in which a record of transactions made in cryptocurrencies are maintained across computers linked in a peer-to-peer network

Gas : Fees that need to be paid in ether to miners in order to facilitate transactions and execute smart contracts.

State clearing : Removal of empty accounts to reduce time of syncing on the network