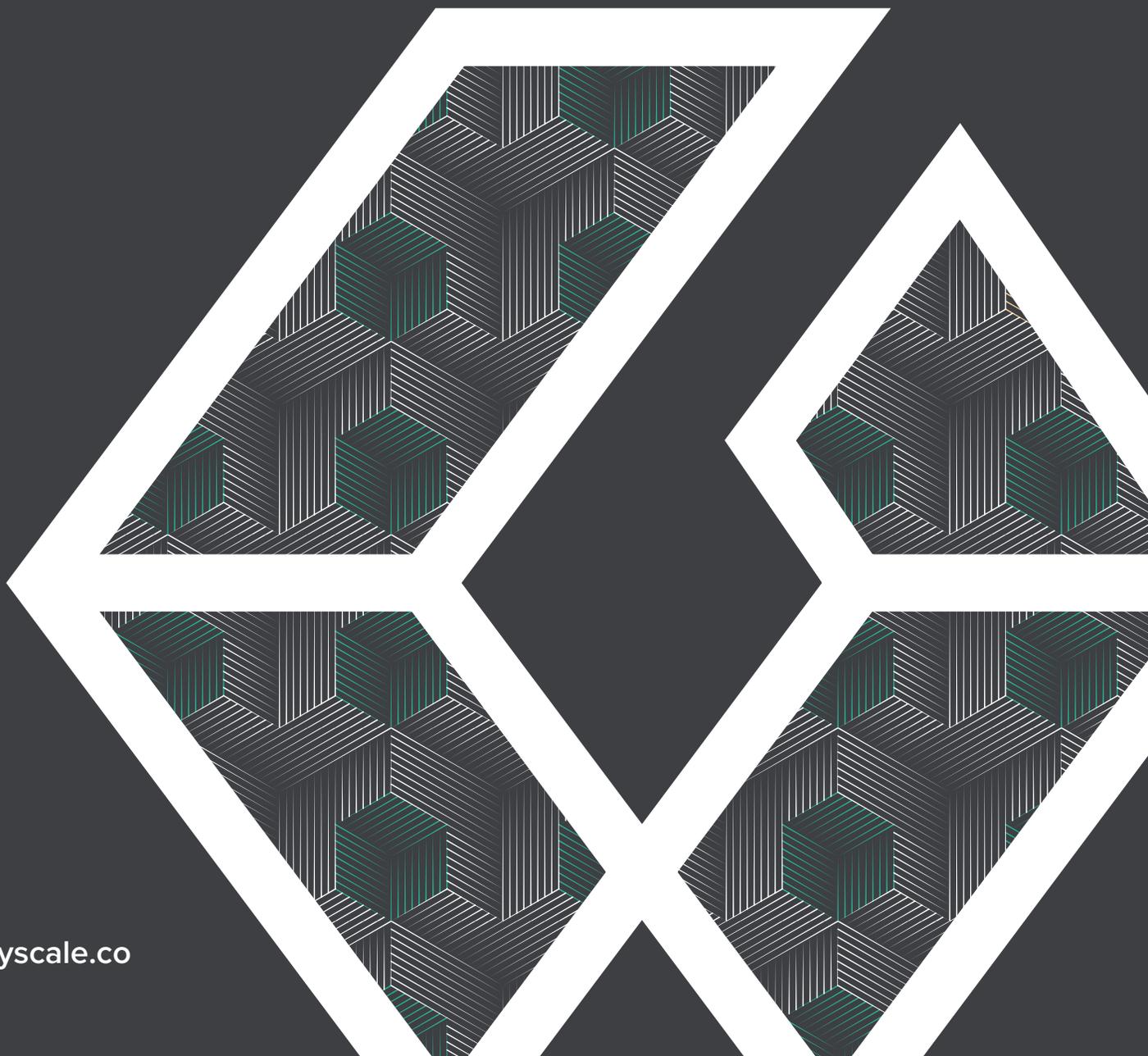


# An Introduction to Ethereum



# An Introduction to Ethereum

Ethereum is a global, open-source blockchain platform for decentralized applications (DApps), powered by smart contracts and embedded with a native digital currency, ether (ETH).<sup>1</sup> On Ethereum, code can be written to control the transmission of digital value based on programmable conditions. Ether serves three main purposes: (i) to store value in ETH, (ii) to settle transactions by allowing users to send or receive payments in ETH and (iii) to facilitate network operations (i.e., power DApps) via transaction fees paid in ETH, which are based on the computational costs of executing the code. Ethereum was conceptualized through a [whitepaper](#) published in November 2013 by Vitalik Buterin, and with additional contributions from his seven co-founders<sup>2</sup> and other developers, the network was launched in June 2015. Initial development was led by the since dissolved Ethereum Switzerland GmbH (EthSuisse), and is currently overseen by the Ethereum Foundation, a non-profit organization based in Switzerland.<sup>3</sup>

Prior to inception, Ethereum was designed to expand upon Bitcoin's primary function as a peer-to-peer (P2P) digital currency, by incorporating a platform capable of deploying smart contracts and more complex structures, such as DApps and decentralized autonomous organizations (DAOs).<sup>4</sup> Its progress is driven by the collaborative efforts of its global developer community, recognized as the largest amongst all digital currency networks.<sup>5</sup> Currently, Ethereum is in its fourth stage of development, called Serenity or Ethereum 2.0, which will be rolled out in several phases, with completion expected sometime after 2022.<sup>6</sup>

1. Ethereum.org. <https://ethereum.org/>.

2. Along with Vitalik Buterin, the Ethereum co-founders in alphabetical order are: Mihai Alisie, Amir Chetrit, Charles Hoskinson, Joseph Lubin, Anthony Di Iorio, Jeffrey Wilke, and Dr. Gavin Wood.

3. "Ethereum Foundation." *EthHub*. <https://docs.ethhub.io/ethereum-basics/ethereum-foundation/>.

4. Decentralized applications (DApps) are applications, programs, or tools that utilize smart contracts built into the Ethereum network. Decentralized Autonomous Organizations (DAOs) are organizations that function independent of a central governing body, and are an autonomous application of a DApp.

5. Ethereum.org. <https://ethereum.org/what-is-ethereum/>.

6. "The Roadmap to Serenity." *Consensys*. May 16, 2019. <https://media.consensys.net/the-roadmap-to-serenity-bc25d5807268>.



FIGURE 1: **ETHEREUM SUMMARY STATISTICS**<sup>7</sup>

As of February 12, 2020

Asset	Ether (ETH)
Inception of Network	July 30, 2015
Price (USD)	\$265.41
Market Cap (USD)	\$29.1 billion
Circulating Supply (ETH % of Year 2050 Estimated Supply)	109.7 million / 81.2%
Year 2050 Estimated Supply (ETH) <sup>8</sup>	Approximately 135.1 million
Current Mining Block Reward (ETH) <sup>9</sup>	2 ETH
Current Annual Inflation Rate <sup>10</sup>	Approximately 4.5%
Average Block Time <sup>11</sup>	Approximately 13 seconds
Market Segment	Digital Currency Smart Contracts General-Purpose Platform

## A Brief History of Ethereum

In the following section, we will briefly cover three major periods in the history of Ethereum: (i) the events leading up to the launch of the network, (ii) the infamous hack of The DAO in June 2016 and (iii) the four planned stages of Ethereum’s recent and future development.

### Part 1: Prior to Network Inception (Early 2013 - July 30, 2015)

Ethereum was first outlined as a proof-of-concept ‘world computer’ in the original 2013 [whitepaper](#) by Vitalik Buterin, an early Bitcoin contributor and co-founder of Bitcoin Magazine. As an early adopter of Bitcoin, Buterin developed the view that a digital currency and its associated blockchain could facilitate much more than simple P2P electronic value transfer. In pursuit of this grander vision, he set out to create a computationally complete virtual ecosystem, featuring a global blockchain and smart contract programming platform. Both would be powered by a native digital currency, ETH.

7. CoinMarketCap.com, Messari / OnChainFX. As of February 12, 2020.

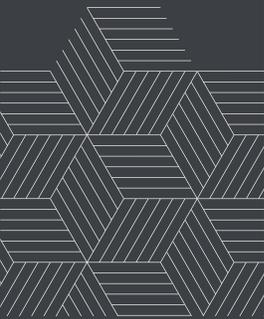
8. ETH does not have max supply. 72 million ETH was created at inception and supply increases in a disinflationary fashion, with new issuance capped at 16 million ETH per year. The inflation rate will ultimately approach zero.

9. “Monetary Policy.” *EthHub*. <https://docs.ethhub.io/ethereum-basics/monetary-policy/>.

10. *Ibid*.

11. Ethereum Average Block Time Chart. *Etherscan*. February 12, 2020. <https://etherscan.io/chart/blocktime>.



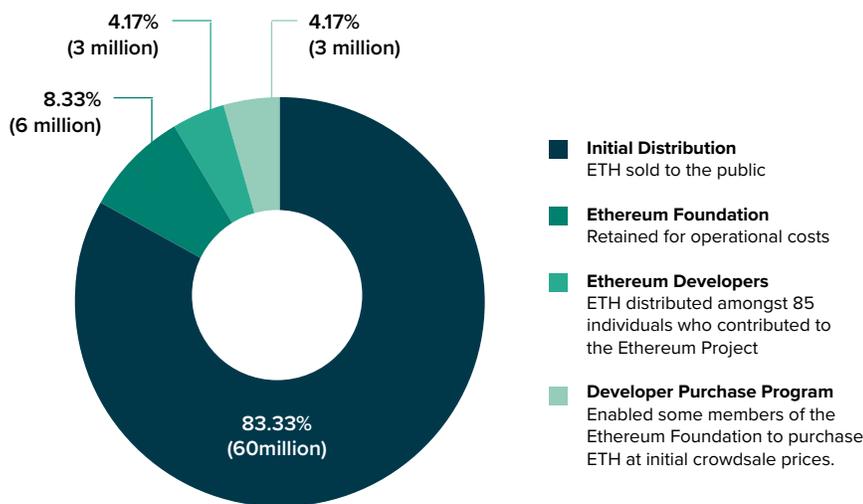


By integrating programming capabilities directly into the Ethereum protocol, developers all over the world would be able to design a new class of decentralized applications hosted on a public blockchain with payment automation using ETH. Through the use of smart contracts, applications built on Ethereum could automate the transmission of information and value under dynamic conditions, enabling tailored business models for a new Internet economy, or Web 3.0.<sup>12</sup>

After joining forces with Mihai Alisie, Amir Chetrit, Charles Hoskinson, Anthony Di Iorio, Dr. Gavin Wood, Joseph Lubin and Jeffrey Wilke in late 2013 and early 2014, Buterin and his colleagues founded Ethereum. Shortly thereafter, Dr. Wood coded the first functional implementation of Ethereum and detailed the technicalities of the protocol, including the Ethereum Virtual Machine (EVM) and smart contract programming language, Solidity, in the [yellow paper](#). On a parallel path, two entities were formed and tasked with overseeing development of Ethereum: EthSuisse, the for-profit arm established in February 2014, and the Ethereum Foundation, its non-profit counterpart established in July 2014.

At network inception on July 30, 2015, 72 million ETH were created and allocated based on the approximate \$18 million USD that was raised in an initial crowdsale, conducted between July and August 2014.<sup>13</sup> Coinciding with the network launch, it was decided that EthSuisse would be dissolved, designating the Ethereum Foundation as the sole organization dedicated to accelerating adoption and usage.

FIGURE 2: ETH SUPPLY ALLOCATION AT INCEPTION<sup>14</sup>

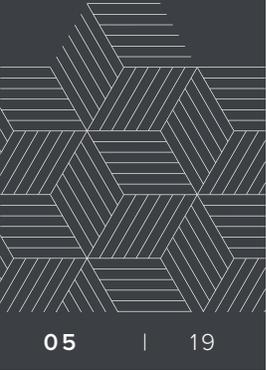


12. Smit Maurya. "Embracing Web 3.0: The New Internet Era Will Begin Soon." *Hacker Noon*. January 22, 2019. <https://hackernoon.com/embracing-web-3-0-the-new-internet-era-will-begin-soon-630ff6c2e7b6>.

13. Amy Castor. "The Ethereum ICO: Where did all the tokens go?" *The Block*. December 18, 2018. <https://www.theblockcrypto.com/2018/12/18/the-ethereum-ico-where-did-all-the-tokens-go/>.

14. Ibid.





## Part 2: The DAO Hack (June 17, 2016)

On April 30, 2016, slock.it, a blockchain and Internet of Things (IoT) solutions company, announced the launch of ‘The DAO’ on Ethereum. The DAO was positioned to function as a decentralized venture capital fund in which over \$150 million USD was raised within a 28-day crowdfunding window.<sup>15</sup> The DAO granted voting rights to members, proportional to their investment, who could then vote to finance projects. If a project proved to be profitable, members would be rewarded based on the terms of the relevant smart contracts and their stake in the DAO.

However, The DAO did not work as planned. On June 17, 2016, an anonymous hacker exploited a bug in the smart contract code used to construct The DAO, siphoning approximately \$60 million worth of ETH into a segregated wallet address. In response, the ETH market experienced a large-scale sell-off as investors rushed to liquidate their holdings.

Controversy ensued within the digital currency community over how to best rectify the situation, given that the stolen funds could not be retrieved. Ultimately, it was decided that a hard fork would take place on July 20, 2016, and a new version of the Ethereum blockchain would be created. This version would be referred to as Ethereum, removing any record of the theft and restoring the stolen ETH to the original owners. The original Ethereum protocol was rebranded as Ethereum Classic, and its native token as ETC. Ethereum Classic left the transaction history untampered, including The DAO theft, in order to preserve the foundational principles of decentralized governance and immutability.

Today, the Ethereum and Ethereum Classic networks coexist and in many ways are just now beginning to interoperate. While similar in functionality and real-world application capabilities, the base-layer separation between these two networks has driven important differences in their technical architectures, development philosophies, and governance principles since the time of the hard fork.

## Part 3: The Four Stages of Ethereum (July 30, 2015 - ?)

Ethereum development has been split into four main stages, with some subdivided into multiple phases. Each stage is integrated into the main protocol as a hard fork, supplemented with comprehensive testing of features in network testnets. Over time, the roadmap has evolved to reflect community consensus. Contributions to the Ethereum Project are made with an eye towards reaching its final stage, Serenity, in which the goal is to be a globally scalable payment network and smart contract platform resistant to centralized governance.

<sup>15</sup> “The DAO of accrue.” *The Economist*. May 19, 2016. <https://www.economist.com/finance-and-economics/2016/05/19/the-dao-of-accrue>.



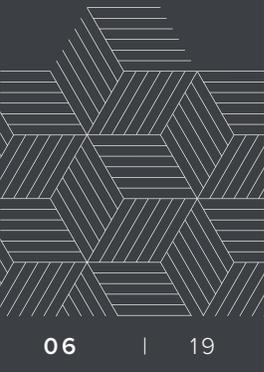
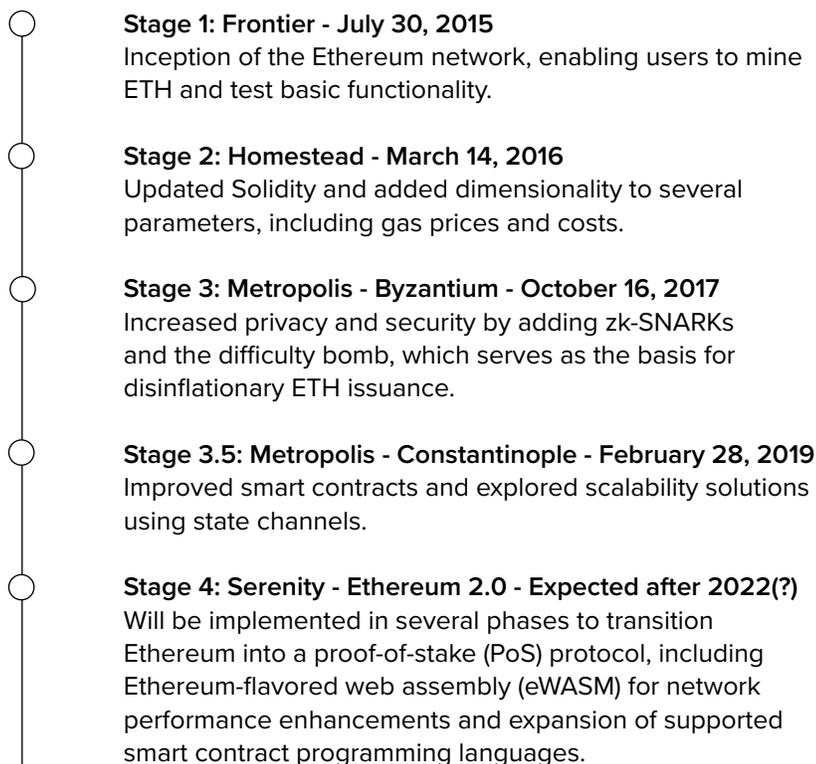


FIGURE 3: THE FOUR STAGES OF ETHEREUM<sup>16</sup>



For a comprehensive explanation of the features introduced in each of the four stages, please refer to [EthHub](#).



16. "A Short History of Ethereum." *Consensus*. May 13, 2019. <https://consensus.net/blog/blockchain-explained/a-short-history-of-ethereum/>.

## Defining Characteristics of Ethereum

The Ethereum network was designed to expand upon the use cases afforded by Bitcoin and serve as a decentralized world computer. While Bitcoin employs a limited scripting language that only permits P2P value transfer, Ethereum was designed to be computationally universal, or Turing-complete, facilitating more advanced types of programmable digital interactions with ETH.

With that said, Ethereum and Bitcoin still share some of the following characteristics, though they are at different points on the spectrum for each:

- **Decentralization:** Ethereum currently employs PoW, effectively eliminating the need for a central authority (e.g., governments and financial institutions) to validate transactions or smart contract-based network operations. Buterin asserts that blockchains are politically and architecturally decentralized, but behave in a logically centralized way, in which the nodes hold equal power in the network and must collaborate to validate transactions.<sup>17</sup>

One caveat is that while governance is designed to be decentralized, there may be risks associated with the level of decentralization of mining pools in the Ethereum network. As of February 12, 2020, the top two largest mining pools controlled over 50% of the hashrate of the network.<sup>18</sup>

- **Permissionless:** Anyone can participate in the network.
- **Secure:** In PoW protocols, the network “is secure as long as honest nodes control more [power] than collective attacker nodes.”<sup>19</sup> An attacker seeking to make a fraudulent transaction on the blockchain would have to locate the desired block, change the transaction data, then mine each consecutive block until the fraudulent one was accepted by the network, in what is called a 51% attack. The primary deterrent of these attacks is that they are computationally expensive with uncertain payoff, and as a result, are unlikely.<sup>20</sup>

Though the 2016 DAO hack raised concerns over Ethereum’s security, Atzei et al. (2016) identified that it was vulnerabilities in Solidity, the programming language used to design Ethereum smart contracts, rather than vulnerabilities in the network itself, as the primary reason for the attack.<sup>21</sup> However, it is important to note that Ethereum will be

17. Vitalin Buterik. “The Meaning of Decentralization.” *Medium*. February 6, 2017. <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>.

18. “Top 25 Miners by Blocks.” *Etherscan*. February 12, 2020. <https://etherscan.io/stat/miner?range=7&blocktype=blocks>.

19. Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Bitcoin Project*. October 31, 2008. <https://bitcoin.org/bitcoin.pdf>.

20. Saravanan Vijayakumaran. “The Security of the Bitcoin Protocol.” *Indian Institute of Technology Bombay*. May 19, 2018. <https://static.zebpay.com/web/pdf/Bitcoin-Security-White-Paper.pdf>.

21. Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. “A survey of attacks on Ethereum smart contracts.” *Università degli Studi di Cagliari*. October 7, 2016. <https://eprint.iacr.org/2016/1007.pdf>.





transitioning from a PoW network security model to a “Proof of Stake” (PoS) network security model in connection with the completion of Serenity. As a material aspect of the Ethereum network, any failure to properly implement such a change could have a material adverse effect on the value of ETH.

- **Open-source:** The source code for the [Ethereum Project](#) is available on the Internet, free for anyone to access, contribute to, or fork. This is an important characteristic for building trust and accumulating users, evidenced by the fact that the Ethereum Project boasts the largest number of active developers out of all digital currency communities.<sup>22</sup>

Users can introduce [Ethereum Improvement Proposals](#) (EIPs), which are feature suggestions designed to improve the network and follow strict technical guidelines.

- **Transparent:** All transactions are recorded and publicly viewable on the Ethereum blockchain from anywhere in the world.
- **Pseudo-anonymous:** Public wallet addresses are not directly linked to any identifying personal information. However, in the current state, complete anonymity is difficult to achieve. This is because addresses involved in any Ethereum transaction are permanently and publicly viewable on the blockchain. Information like multiple transactions originating from one wallet or data leaks from custody solutions or exchanges can almost always trace back to one’s identity.<sup>23</sup>
- **Disinflationary supply:** At inception, 72 million ETH was created. ETH supply increases according to a disinflationary mechanism that will continue to be adjusted as the network matures. However, there is no designated maximum supply cap. An established and transparent monetary supply and issuance schedule is critical for evaluating a digital currency’s long-term investability.



22. Adrian Zmudzinski. “Ethereum Has More Than Twice as Many Core Devs per Month as Bitcoin, Report says.” *Cointelegraph*. March 9, 2019. <https://cointelegraph.com/news/ethereum-has-more-than-twice-as-many-core-devs-per-month-as-bitcoin-report>.  
23. Aaron Van Wirdum. “Is Bitcoin Anonymous? A Complete Beginner’s Guide.” *Bitcoin Magazine*. November 18, 2015. <https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283>.

## Key Features of Ethereum

Ethereum is the first digital asset to incorporate a platform with smart contract capability. It is comprised of the following elements, which are essential to understanding the network and its many applications.

### Ether (ETH)

ETH is the digital currency native to Ethereum. It serves three main purposes: (i) to store value in ETH, (ii) to settle transactions by allowing users to send or receive payments in ETH and (iii) to facilitate network operations (i.e., power DApps) via transaction fees paid in ETH (known as ‘gas’), which are based on the computational costs of executing the code. Gas is the internal unit of value used for smart contract code execution, calculated by measuring the computational cost of executing a given instruction. Miners and smart contract programmers collect transaction fees in ETH, based on the equivalent amount of gas. Gas prices are measured in wei, the smallest unit of ETH, where  $10^{18}$  wei is equal to 1 ETH.

### Smart Contracts

Smart contracts are lines of code that facilitate the exchange of anything representative of value, such as money, information, property, or voting rights. They are uploaded onto the blockchain and transactions executed cannot be modified. Using smart contracts, users can send or receive ETH, create markets, store registries of debts or promises, represent ownership of property or a company, transfer funds given a set of logical instructions, and form new digital assets in compliant offerings or issuances. The concept of a smart contract was first proposed by Nick Szabo, a renowned computer scientist specializing in digital currencies and the creator of Bit Gold, and was explored in his 1997 [whitepaper](#).

### Solidity

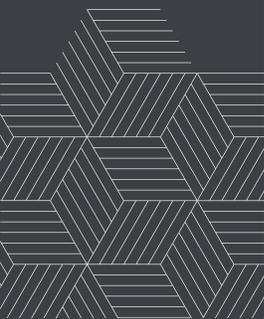
Solidity is the primary programming language of Ethereum. It is used to write smart contracts, develop DApps, structure DAOs, and operate IoT (Internet of Things) devices built on Ethereum technology. Additional languages for the Ethereum network, such as [Vyper](#), are now live while others have been deprecated, like Serpent and Mutan.

### Decentralized Applications (DApps)

DApps are applications, programs, or tools that utilize smart contracts built into the Ethereum network. DApps have potential use cases across many sectors, including financial services, asset management, supply chain management, identity management, and data storage encryption and transfer. Some popular DApps built on the Ethereum blockchain include [MakerDAO](#), [CryptoKitties](#), and [IDEX](#). MakerDAO, in particular, is currently the largest decentralized financing (DeFi) platform.<sup>24</sup> As a tangible application of Ethereum, it has the potential to democratize access to financial services. As of February 12, 2020, approximately 3.1 million ETH were [locked up](#) as collateral for DeFi purposes.

24. “Maker Dominance.” *DeFi Pulse*. February 12, 2020. <https://defipulse.com/>.





### **Decentralized Autonomous Organizations (DAOs)**

Decentralized Autonomous Organizations (DAOs) are organizations that function independent of a central governing body. Unlike traditional companies where ownership is divided amongst shareholders, a DAO is owned by those who contribute tokens, who are also given voting rights. In addition, the rules of a DAO are determined by its accompanying collection of smart contracts.

### **Ethash Algorithm**

Although both Ethereum's Ethash and Bitcoin's SHA-256 utilize PoW, the two protocols differ in how they address ASICs (Application-Specific Integrated Circuits). In Ethash, GPUs (Graphical Processing Units) are the preferred choice of equipment and are relatively cheaper compared to ASICs, which are integral to SHA-256. As a result, the Ethereum mining process is more egalitarian with a lower cost barrier to entry. It also reduces the probability of mining centralization, and subsequent risk of attacks on the network. However, the tradeoff for adopting Ethash is that computations are more memory intensive.<sup>25</sup>

For more on the technicalities on Ethash, please refer to this open-source [guide](#) on Github.

### **Ethereum Virtual Machine (EVM)**

The EVM was created by Dr. Gavin Wood in 2014 and detailed in the original Ethereum [yellow paper](#), the technical version of the whitepaper. A virtual machine (VM) is software that emulates the behavior of a computer, essentially acting as a runtime environment for any activity that one can perform on a regular computer.<sup>26</sup> It allows users to test features and eliminates the risk of attacks and failures on the main computer hosting a VM, or multiple VMs as allowed by memory constraints. If an attack were to be carried out on a VM and certain functions are compromised, the user simply needs to exit the VM.

The EVM handles the state of the Ethereum blockchain and executes all smart contracts, DApps, and DAOs on the network. It is Turing complete, meaning that the program will always run to completion given sufficient time and memory. This was a significant innovation in blockchain technology because it permitted sophisticated, conditional logic and provides the basis for more complex programs. Other virtual machines, such as [SputnikVM](#), are in development and increasingly utilized in Ethereum blockchain projects.

25. Vitalik Buterin. "On Mining." *Ethereum Foundation Blog*. June 19, 2014. <https://blog.ethereum.org/2014/06/19/mining/>.  
26. "What is a virtual machine?" *Microsoft Azure*. <https://azure.microsoft.com/en-us/overview/what-is-a-virtual-machine/>.



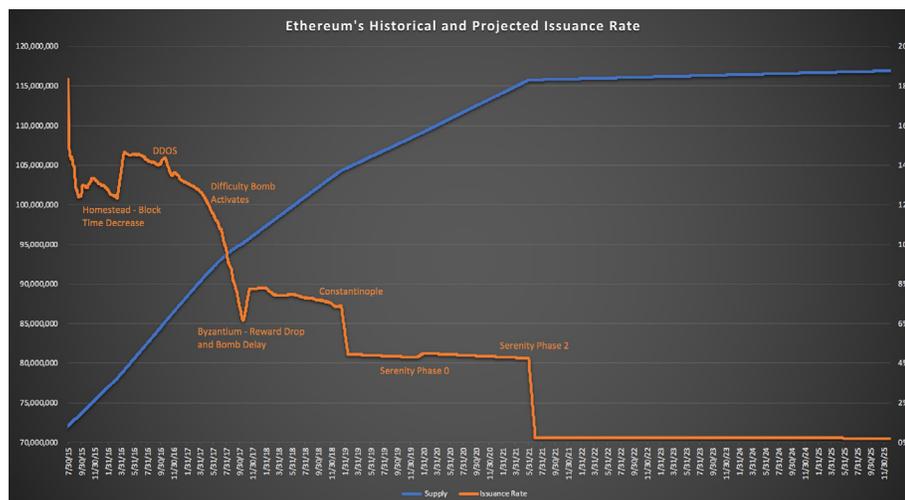


## Mining Rewards

At inception, 72 million ETH were created and distributed to the public, the Ethereum Foundation, and developers in an initial crowdsale as specified in Figure 2. Ethereum is equipped with a disinflationary mechanism to control the rate of new ETH supply issuance, which is currently capped at an additional 16 million ETH a year. The intuition behind this was to prevent arbitrary creations of money, potentially leading to hyperinflation or manipulation.

Miners who successfully confirm a transaction and upload it to the blockchain receive block rewards for their effort, providing an incentive and attributing to the exponential increase in network usage. Block rewards began at 5 ETH, decreased to 3 ETH after the Byzantium hard fork, and decreased to the current reward of 2 ETH after the Constantinople hard fork.<sup>27</sup> Like Bitcoin, Ethereum miners may also be paid additional amounts of ETH to account for transaction fees.

FIGURE 4: ETHEREUM PROPOSED MINING REWARD TIMELINE<sup>28</sup>



Since inception, the history of block rewards is as follows<sup>29</sup>:

- Block #0 to Block #4,369,999: 5 ETH
- Block #4,370,000 to Block #7,280,000: 3 ETH (changed via [EIP-649](#))
- Block #7,280,000 to now: 2 ETH (changed via [EIP-1234](#))

27. "The Thirddening: What You Need to Know." *Consensys*. January 10, 2019. <https://media.consensys.net/the-thirddening-what-you-need-to-know-df96599ad857>.

28. "Monetary Policy." *EthHub*. <https://docs.ethhub.io/ethereum-basics/monetary-policy/>.

29. "Monetary Policy." *EthHub*. <https://docs.ethhub.io/ethereum-basics/monetary-policy/>.



## Potential Advantages to Ethereum

The design of the Ethereum protocol leads to three potential advantages when compared to traditional financial institutions, payment channels, and other digital currency networks:

- 1. Pioneering smart contract capability:** Ethereum was the first digital currency network to incorporate a platform for smart contracts. Given this functionality, real-world use cases are already beginning to emerge and sustain value (e.g., Decentralized Finance or DeFi). Considering Ethereum's position as the second largest digital currency network over the past several years, it's important to recognize its influence within the digital asset class and on traditional finance.
- 2. Active developer community:** Ethereum is one of the most popular digital currency networks across all metrics for Github activity, including number of commits, total contributors, total project watchers, and total stars.<sup>30</sup>
- 3. Institutional and enterprise support:** The Enterprise Ethereum Alliance (EEA) is an organization dedicated to promoting Ethereum adoption and usage for both companies and individuals. It also seeks to build enterprise blockchain solutions and potentially private, federated versions of Ethereum's blockchain to address previously unmet business needs.<sup>31</sup> It is made up of over 450 multinational companies, including Microsoft, JP Morgan, Toyota, and Intel. The growing number of firms joining the EEA is representative of a trend where established firms are now exploring the value of blockchain technology and investing significant time and resources towards related initiatives.

## Potential Risks of Ethereum

There are important trade offs to consider when choosing between different digital currency networks to use and invest in. Selection will often depend on the one that best satisfies the needs of the user. Below we outline four key risks related to investing in Ethereum:

### Scalability Problems

Like many of its digital currency counterparts, Ethereum faces limitations in terms of scalability. Currently, the network can only process an average of 15 transactions per second, compared to traditional payment channels such as VISA, which handles approximately 1,700 transactions per second (and claims to have the capacity to handle more than 24,000 per second).<sup>32</sup> Ethereum

30. "Cryptocurrency Development Activity and Ranking." *CoinCodeCap*. As of February 12, 2020. <https://coincodcap.com/>.

31. Enterprise Ethereum Alliance. <https://entethalliance.org/>.

32. Visa. February 12, 2020. <https://usa.visa.com/run-your-business/small-business-tools/retail.html>.





has already undergone several software modifications to adapt to the scaling challenges presented by its initial design. However, scalability continues to be one of the largest challenges for the Ethereum network and remains an active area of research for developers.

There are two types of approaches being researched to resolve Ethereum's scalability issues: (i) on-chain, or Layer 1, which refers to the main blockchain and (ii) off-chain, or Layer 2, which refers to feature implementations outside of the main blockchain, such as Plasma, Sidechains, Payment Channels, and State Channels.

For more on planned scalability features for Ethereum 2.0, please refer to the [Ethereum](#) Github.

### **Level of Decentralization**

There may be risks associated with the level of decentralization of the Ethereum network, particularly with respect to mining pools. For example, as of February 12, 2020, the top two largest mining pools controlled over 50% of the network hashrate.<sup>33</sup>

### **Competition**

Ethereum faces strong competition from a broad spectrum of general-purpose platform digital currency networks, including Ethereum Classic, Horizen, Eos, and Tezos, among others. Each of these may be viewed as direct or indirect competitors to Ethereum and it remains to be seen whether DApps, smart contract functionality, or other use cases may be better served on one or some versus others. It is also possible that these networks fail collectively, or that some combination of them succeed alongside one another due to competitive market forces. However, Ethereum generally has higher rates of adoption compared to the competitive networks mentioned (and others), extending to developers, exchange listings, applications, and basic network infrastructure, such as wallet- and front-end payment processing-software.

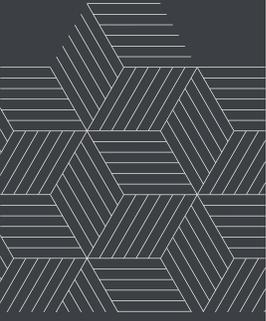
### **Volatility with Smart Contracts**

Since transactions resulting from smart contracts may be difficult to stop or reverse, any vulnerabilities in the underlying code can weaken the network. For example, the 2016 exploit in The DAO allowed an unknown attacker to siphon approximately \$60 million worth of ETH into a segregated wallet address. This event spurred the controversial hard fork of Ethereum, resulting in its split into two networks: Ethereum and Ethereum Classic. In 2017, Parity, the multi-sig wallet software created by Parity Technologies, was affected by two hacks. The first, in July 2017, resulted in a theft of \$30 million in ETH, and the second, in November 2017, led to an indefinite freeze of approximately \$160 million in ETH.<sup>34</sup> Smart contract technology is relatively new and still in open-source development.

33. "Top 25 Miners by Blocks." *Etherscan*. February 12, 2020. <https://etherscan.io/stat/miner?range=7&blocktype=blocks>.

34. Jon Russell. "A major vulnerability has frozen hundreds of millions of dollars of Ethereum." *TechCrunch*. November 7, 2017. <https://techcrunch.com/2017/11/07/a-major-vulnerability-has-frozen-hundreds-of-millions-of-dollars-of-ethereum/>





### **Monetary Policy Concerns**

ETH does not have a maximum supply cap and the monetary policy roadmap appears somewhat ambiguous. Proposals have been introduced, recommending that the Ethereum network install a supply cap to introduce monetary scarcity and prevent arbitrary creations of money. In particular, in [EIP 960](#), Buterin suggested a supply limit cap of 120 million ETH, but this has not been accepted by the general community.

### **Regulatory Uncertainty**

The SEC has stated that certain digital assets may be considered “securities” under the federal securities laws. To date, the SEC has only identified two digital assets, Bitcoin and Ethereum, for which it does not intend to take the position that they are securities. However, there are a number of regulatory considerations related to tokens, products, and businesses built atop the open-source Ethereum network that could pose further risks to ETH prices.

## **Summary**

Ethereum initiated the second wave of innovation in blockchain technology, expanding upon the use cases afforded by Bitcoin and solidifying its own unique role in the digital currency ecosystem. In its final form, Ethereum seeks to be the leading smart contract-compatible digital currency platform. Despite the 2016 DAO hack that resulted in the controversial Ethereum-Ethereum Classic hard fork, Ethereum maintains its position as the second largest network by market cap in the digital currency ecosystem and has proven resilient with an extensive following of supporters. With its global network of users, developers, and enterprises, Ethereum has generated significant technological and social momentum that will be difficult for competing platforms to replicate.

To learn more about other digital assets underpinning the Grayscale family of products, please visit the Building Blocks section of [Grayscale Insights](#).





## About Grayscale Investments, LLC

Grayscale Investments is the world's largest digital currency asset manager. With a proven track record and unrivaled experience, we give investors the tools to make informed investing decisions in a burgeoning asset class. As part of Digital Currency Group, Grayscale accesses the world's biggest network of industry intelligence to build better investment products. We have removed the barrier to entry so that institutions and individual investors can benefit from exposure to digital currencies. Now, forward-thinking investors can embrace a digital future with an institutional grade investment.

Grayscale is headquartered in New York City. For more information on Grayscale, please visit [www.grayscale.co](http://www.grayscale.co) or follow us on Twitter [@GrayscaleInvest](https://twitter.com/GrayscaleInvest).



## Important Disclosures & Other Information

©Grayscale Investments, LLC. All content is original and has been researched and produced by Grayscale Investments, LLC (“Grayscale”) unless otherwise stated herein. No part of this content may be reproduced in any form, or referred to in any other publication, without the express consent of Grayscale.

This paper is for informational purposes only and does not constitute an offer to sell or the solicitation of an offer to sell or buy any security in any jurisdiction where such an offer or solicitation would be illegal. There is not enough information contained in this paper to make an investment decision and any information contained herein should not be used as a basis for this purpose. This paper does not constitute a recommendation or take into account the particular investment objectives, financial situations, or needs of investors. Investors are not to construe the contents of this paper as legal, tax or investment advice, and should consult their own advisors concerning an investment in digital assets. The price and value of assets referred to in this research and the income from them may fluctuate. Past performance is not indicative of the future performance of any assets referred to herein. Fluctuations in exchange rates could have adverse effects on the value or price of, or income derived from, certain investments.

Investors should be aware that Grayscale is the sponsor of Grayscale Bitcoin Trust (BTC), Grayscale Bitcoin Cash Trust (BCH), Grayscale Ethereum Trust (ETH), Grayscale Ethereum Classic Trust (ETC), Grayscale Litecoin Trust (LTC), Grayscale Horizen Trust (ZEN), Grayscale Stellar Lumens Trust (XLM), Grayscale XRP Trust (XRP) and Grayscale Zcash Trust (ZEC) (each, a “Trust”) and the manager of Grayscale Digital Large Cap Fund LLC (the “Fund”). The Trusts and the Fund are collectively referred to herein as the “Products”. Any Product currently offering Share creations is referred to herein as an “Offered Product”. Information provided about an Offered Product is not intended to be, nor should it be construed or used as investment, tax or legal advice, and prospective investors should consult their own advisors concerning an investment in such Offered Product. This paper does not constitute an offer to sell or the solicitation of an offer to buy interests in any of the Products. Any offer or solicitation of an investment in a Product may be made only by delivery of such Product’s confidential offering documents (the “Offering Documents”) to qualified accredited investors (as defined under Rule 501(a) of Regulation D of the U.S. Securities Act of 1933, as amended), which contain material information not contained herein and which supersede the information provided herein in its entirety.

The Products are private investment vehicles. Shares of Grayscale Bitcoin Trust (BTC), which are only offered on a periodic basis, are publicly quoted under the symbol: GBTC. The Products are not subject to the same regulatory requirements as exchange traded funds or mutual funds, including the requirement to provide certain periodic and standardized pricing and valuation information to investors. The Products are not registered with the Securities and Exchange Commission (the “SEC”), any state securities laws, or the U.S. Investment Company Act of 1940, as amended. There are substantial risks in investing in one or more Products. Any interests in each Product described herein have not been recommended by any U.S. federal or state, or non-U.S., securities commission or regulatory authority, including the SEC. Furthermore, the foregoing authorities have not confirmed the accuracy or determined the adequacy of this document. Any representation to the contrary is a criminal offense.

Certain of the statements contained herein may be statements of future expectations and other forward-looking statements that are based on Grayscale’s views and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in such statements. In addition to statements that are forward-looking by reason of context, the words “may, will, should, could, can, expects, plans, intends, anticipates, believes, estimates, predicts, potential, projected, or continue” and similar expressions identify forward-looking statements. Grayscale assumes no obligation to update any forward-looking statements contained herein and you should not place undue reliance on such statements, which speak only as of the date hereof. Although Grayscale has taken reasonable care to ensure that the information contained herein is accurate, no representation or warranty (including liability towards third parties), expressed or implied, is made by Grayscale as to its accuracy, reliability or completeness. You should not make any investment decisions based on these estimates and forward-looking statements.

[PLEASE REVIEW IMPORTANT DISCLOSURES & OTHER INFORMATION AT THE END OF THIS PAPER.](#)

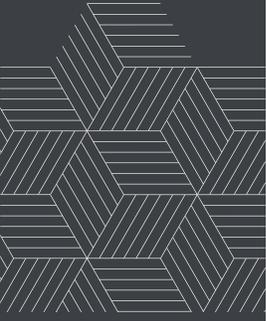


## Certain Risk Factors

Each Product is a private, unregistered investment vehicle and not subject to the same regulatory requirements as exchange traded funds or mutual funds, including the requirement to provide certain periodic and standardized pricing and valuation information to investors. There are substantial risks in investing in a Product or in digital assets directly, including but not limited to:

- **PRICE VOLATILITY**  
Digital assets have historically experienced significant intraday and long-term price swings. In addition, none of the Products currently operates a redemption program and may halt creations from time to time or, in the case of Grayscale Bitcoin Trust (BTC), periodically. There can be no assurance that the value of the common units of fractional undivided beneficial interest (“Shares”) of any Product will approximate the value of the digital assets held by such Product and such Shares may trade at a substantial premium over or discount to the value of the digital assets held by such Product. At this time, none of the Products is operating a redemption program and therefore Shares are not redeemable by any Product. Subject to receipt of regulatory approval from the SEC and approval by Grayscale, in its sole discretion, any Product may in the future operate a redemption program. Because none of the Products believes that the SEC would, at this time, entertain an application for the waiver of rules needed in order to operate an ongoing redemption program, none of the Products currently has any intention of seeking regulatory approval from the SEC to operate an ongoing redemption program.
- **MARKET ADOPTION**  
It is possible that digital assets generally or any digital asset in particular will never be broadly adopted by either the retail or commercial marketplace, in which case, one or more digital assets may lose most, if not all, of its value.
- **GOVERNMENT REGULATION**  
The regulatory framework of digital assets remains unclear and application of existing regulations and/or future restrictions by federal and state authorities may have a significant impact on the value of digital assets.
- **SECURITY**  
While each Product has implemented security measures for the safe storage of its digital assets, there have been significant incidents of digital asset theft and digital assets remains a potential target for hackers. Digital assets that are lost or stolen cannot be replaced, as transactions are irrevocable.
- **TAX TREATMENT OF VIRTUAL CURRENCY**  
For U.S. federal income tax purposes, Digital Large Cap Fund will be a passive foreign investment company (a “PFIC”) and, in certain circumstances, may be a controlled foreign corporation (a “CFC”). Digital Large Cap Fund will make available a PFIC Annual Information Statement that will include information required to permit each eligible shareholder to make a “qualified electing fund” election (a “QEF Election”) with respect to Digital Large Cap Fund. Each of the other Products intends to take the position that it is a grantor trust for U.S. federal income tax purposes. Assuming that a Product is properly treated as a grantor trust, Shareholders of that Product generally will be treated as if they directly owned their respective pro rata shares of the underlying assets held in the Product, directly received their respective pro rata shares of the Product’s income and directly incurred their respective pro rata shares of the Product’s expenses. Most state and local tax authorities follow U.S. income tax rules in this regard. Prospective investors should discuss the tax consequences of an investment in a Product with their tax advisors.
- **NO SHAREHOLDER CONTROL**  
Grayscale, as sponsor of each Trust and the manager of the Fund, has total authority over the Trusts and the Fund and shareholders’ rights are extremely limited.
- **LACK OF LIQUIDITY AND TRANSFER RESTRICTIONS**  
An investment in a Product will be illiquid and there will be significant restrictions on transferring interests in such Product. The Products are not registered with the SEC, any state securities laws, or the U.S. Investment Company Act of 1940, as amended, and the Shares of each Product are being offered in a private placement pursuant to Rule 506(c)





under Regulation D of the Securities Act of 1933, as amended (the “Securities Act”). As a result, the Shares of each Product are restricted Shares and are subject to a one-year holding period in accordance with Rule 144 under the Securities Act. In addition, none of the Products currently operates a redemption program. Because of the one-year holding period and the lack of an ongoing redemption program, Shares should not be purchased by any investor who is not willing and able to bear the risk of investment and lack of liquidity for at least one year. No assurances are given that after the one year holding period, there will be any market for the resale of Shares of any Product, or, if there is such a market, as to the price at such Shares may be sold into such a market.

- **POTENTIAL RELIANCE ON THIRD-PARTY MANAGEMENT; CONFLICTS OF INTEREST**

The Products and their sponsors or managers and advisors may rely on the trading expertise and experience of third-party sponsors, managers or advisors, the identity of which may not be fully disclosed to investors. The Products and their sponsors or managers and advisors and agents may be subject to various conflicts of interest.

- **FEES AND EXPENSES**

Each Product’s fees and expenses (which may be substantial regardless of any returns on investment) will offset each Product’s trading profits.

### **Additional General Disclosures**

Investors must have the financial ability, sophistication/experience and willingness to bear the risks of an investment. This document is intended for those with an in-depth understanding of the high risk nature of investments in digital assets and these investments may not be suitable for you. This document may not be distributed in either excerpts or in its entirety beyond its intended audience and the Products and Grayscale will not be held responsible if this document is used or is distributed beyond its initial recipient or if it is used for any unintended purpose.

The Products and Grayscale do not: make recommendations to purchase or sell specific securities; provide investment advisory services; or conduct a general retail business. None of the Products or Grayscale, its affiliates, nor any of its directors, officers, employees or agents shall have any liability, howsoever arising, for any error or incompleteness of fact or opinion in it or lack of care in its preparation or publication, provided that this shall not exclude liability to the extent that this is impermissible under applicable securities laws.

The logos, graphics, icons, trademarks, service marks and headers for each Product and Grayscale appearing herein are service marks, trademarks (whether registered or not) and/or trade dress of Grayscale Investments, LLC. (the “Marks”). All other trademarks, company names, logos, service marks and/or trade dress mentioned, displayed, cited or otherwise indicated herein (“Third Party Marks”) are the sole property of their respective owners. The Marks or the Third Party Marks may not be copied, downloaded, displayed, used as metatags, misused, or otherwise exploited in any manner without the prior express written permission of the relevant Product and Grayscale or the owner of such Third Party Mark.

The above summary is not a complete list of the risks and other important disclosures involved in investing in any Product or digital assets and is subject to the more complete disclosures contained in each Product’s Offering Documents, which must be reviewed carefully.





## **General Inquiries:**

info@grayscale.co

Address: 250 Park Ave S 5th floor, New York, NY 10003

Phone: (212) 668-1427

@GrayscaleInvest