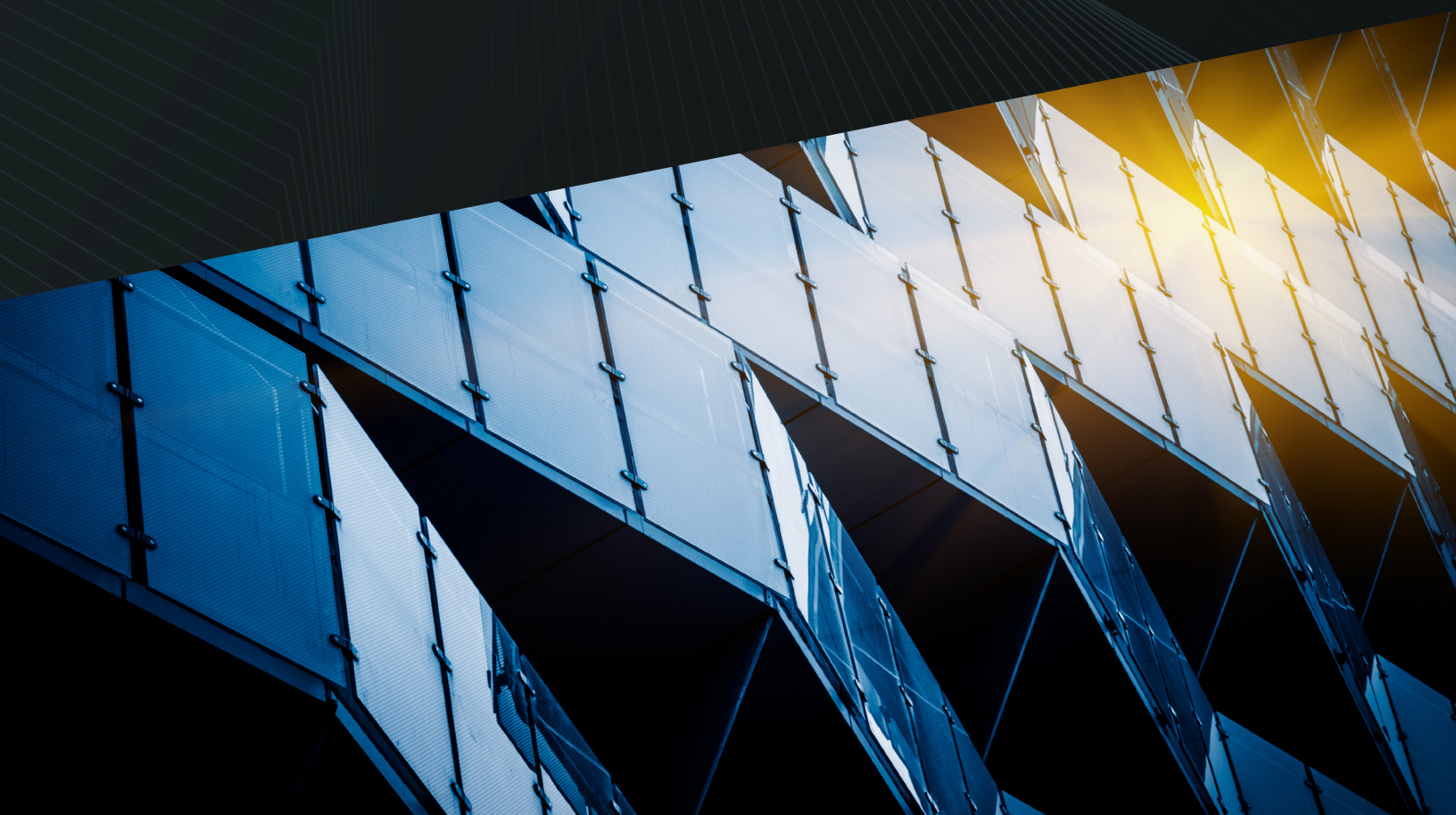
Fidelity DIGITAL ASSETS℠

MAY 2022

Ethereum

Advancing blockchain with smart contracts and decentralized applications

Chris Kuiper, CFA® – Director of Research, Fidelity Digital Assets℠
Jack Neureuter – Research Analyst, Fidelity Digital Assets℠



Introduction

In the years following the invention and launch of bitcoin in 2009, digital assets largely represented a single value proposition. Most non-bitcoin tokens launched in the years after offered what many industry analysts have characterized as an inferior and undifferentiated version of bitcoin's value proposition.[1] That perception in the marketplace changed in 2015 with the release of the Ethereum protocol. A digital asset exhibiting alternative value propositions to bitcoin and a wide array of potential use cases emerged. This launch spawned a new era in digital assets featuring increased innovation, competition, and tradeoffs as well as new potential use cases.

This paper will introduce the Ethereum ecosystem and is intended as a primer for those interested in learning about the basics of Ethereum and its potential investment thesis. Specifically, this paper will cover what Ethereum is, some of its history, its value proposition, and risks. We believe it would be very beneficial for readers to have an understanding of Bitcoin as a foundation before exploring Ethereum in detail, so we provide background on some of Bitcoin's key features as a point of comparison throughout the paper to help explain what we believe Ethereum is and isn't.

The points below highlight some of our main takeaways:

- Ethereum is a digital asset network whose main value proposition is derived from its programmability. Ethereum features an open-ended architecture in hopes of attracting developers able to build useful applications and drive demand for use of the Ethereum network and its native token, ether.
- Fidelity Digital Assets does not consider the Ethereum and Bitcoin networks to exist within the same category. We believe the Bitcoin network is best understood as fulfilling a monetary use case, while the Ethereum network has made tradeoffs to compete for other potential use cases.
- The Ethereum roadmap is ambitious, with plans this year and next to move to a new consensus mechanism as well as plans to improve scaling. This may bring about large improvements and open the ecosystem to new opportunities as well as large risks.

1 For example, even Vitalik Buterin in a defense of "altcoins" written in 2013, pointed out that critics of non-bitcoin tokens were missing the biggest critique of these alternatives – that most "offer essentially no value over Bitcoin itself." Buterin, Vitalik. "In Defense of Alternative Cryptocurrencies." *Bitcoin Magazine*. B.TC Inc, September 7, 2013. https://bitcoinmagazine.com/business/defense-alternative-cryptocurrencies.

What is Ethereum?

A Programmable Blockchain

The Bitcoin network was the first to successfully launch a decentralized, peer-to-peer, open-source, distributed network that could facilitate transactions of digitally scarce tokens, thereby acting like a payment network. This, combined with Bitcoin's transparent and immutable ledger (or database), is known as a specific type of decentralized ledger technology, called blockchain technology. Ethereum's creators recognized the significance of Bitcoin's breakthrough, but also the potential to extend the technology by making a blockchain *programmable* or with enhanced functionality.

What Ethereum Enables – The Rise of Decentralized Apps (dApps)

This enhanced functionality provides the ability to create decentralized applications, or applications that can run without relying on one computer, service provider, or cloud server. Like the Bitcoin network, the Ethereum network is made up of many computers all running the same code or software. For decentralized applications this means that instead of centralized cloud servers running applications for users to access online, this is replaced with many smaller computers all running the same Ethereum software that then powers the applications built on top of this network.

Since the Ethereum network is decentralized, all applications built on top of it are also decentralized (no one person controls it) and permissionless (anyone can plug into the network to build and run applications). While some of the decentralized applications running on Ethereum may look and operate the same as current applications that use a more centralized system (such as an instant message or chat service), the fact that the application is more decentralized means it is much harder to exclude people from accessing the application or shutting it down.

What are Smart Contracts?

Ethereum's programmability allows for the creation of smart contracts, or computer programs that reside on the Ethereum blockchain.[2] These smart contracts are the building blocks of the different functions and decentralized applications that can be built on the Ethereum network. Later we will examine some of the use cases that smart contracts enable, such as decentralized finance and stablecoins.

The term "smart contract" was coined in 1994 by Nick Szabo in a paper by the same name[3] where he defined a smart contract as "a computerized transaction protocol that executes the terms of a contract."

2 "Introduction to Smart Contracts." ethereum.org, January 10, 2022. https://ethereum.org/en/developers/docs/smart-contracts/.

3 Szabo, Nick. "Smart Contracts." University of Amsterdam, 1994. Accessed April 12, 2022. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

Smart contracts are therefore similar to law contracts, or even just casual agreements, where if a certain condition is met then there is a predetermined output or transaction. However, there are some interesting differences between digital smart contracts and traditional agreements:

Traditional Contracts or Agreement	Smart Contracts
Need to trust the other party to fulfill obligation	No need to trust the other party, obligation automatically executes when certain conditions are met. However, this also introduces the risk of automatic execution of unintended action (e.g. mis-programmed code)
Risk of unpredictable outcome, such as human judges interpreting contracts differently	Only one interpretation by the computer reading the code
May not be public or verifiable	Smart contracts reside on the blockchain, making them auditable and transparent, but may therefore sacrifice privacy in some cases
May have lower privacy (contracts tied to individual identity)	Ethereum is a pseudonymous network, so transactions are tied to a unique address but not necessarily a person's identity
Risk of fraud, unauthorized contract alterations, or misrepresentation of parties in contracts	Risk of bugs in smart contract code and therefore potential exploits or hacks of the code

Vending Machines as a Smart Contract Example

A classic example used to describe smart contracts is a digital vending machine.[4] A vending machine is just a machine with pre-programmed logic of if-this-then-that structure. If you select a product, then insert the correct amount of money, the machine will dispense the product. If you do not do these things, it will not dispense the product. Notice that like smart contracts, once it is programmed, there is no other human operation or verification needed for it to run. Also like smart contracts, if the vending machine is incorrectly programmed, there could be a different result than originally desired (such as dispensing ten products, instead of just one for a certain price).

What is Ether (ETH)?

Ethereum's native currency is known as ether or ETH[5], similar to how the Bitcoin protocol's native currency is the bitcoin token. Payment along the Ethereum network is always required to be made in the protocol's native token, ether, regardless of whether you want to make simple peer-to-peer payments or execute more complex smart contract-reliant transactions. These transaction fees are often referred to as "gas fees"[6] and represent the required payment to miners for ensuring a safe disintermediated transaction, similar to how transaction fees are paid to miners on the Bitcoin network. The requirement for ether to be involved in the facilitation of every single network transaction creates a potential linkage between developers building useful applications and the ether token accruing value.

4 Szabo, Nick. "Smart Contracts." University of Amsterdam, 1994. Accessed April 12, 2022. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

5 "What Is Ether (ETH)?" ethereum.org. April 4, 2022. https://ethereum.org/en/eth/.

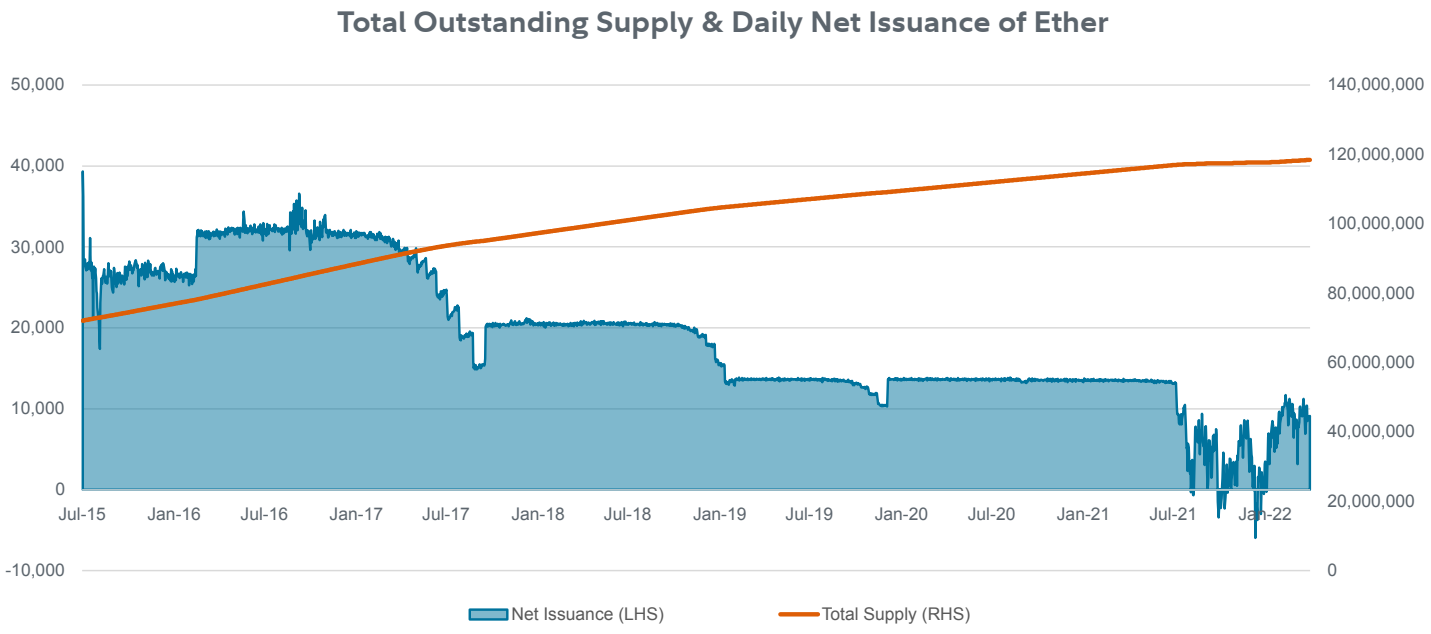
6 "Gas and Fees." ethereum.org, March 9, 2022. https://ethereum.org/en/developers/docs/gas/.

A Refresher on "Miners"

The Bitcoin and Ethereum blockchain networks are distributed and decentralized, meaning they are made up of many computers running the same code, but with no one person or institution in charge. They therefore rely on "miners" to help secure this network and achieve consensus among the participants. Miners provide two main functions. The first is to confirm transactions to the blockchain database or record. To do this the miners must expend electricity and computing power. This expenditure leads to the second function of miners, which is to secure the network from attackers. For example, someone who would want to change the record or database to enrich themselves would need to outspend the miners in terms of electricity and computing power, an increasingly difficult thing to do as the network's computing power increases. For this expenditure, miners are rewarded with newly issued tokens, such as bitcoin or ether.

The Ether Issuance Schedule

Ethereum's issuance schedule of new ether is not fixed, but rather follows a "minimum viable issuance."[7] Ethereum's future issuance schedule revolves around keeping miners incentivized to securely validate transactions on the network. As a result, the future issuance policy of ether is largely unknown. To date, the issuance rate has been reduced multiple times. The addition of burning ETH, as part of a recent upgrade, has resulted in days where the net issuance of ETH is negative (more ETH is burned than minted). Burning is simply the act of sending a specific amount of tokens to a wallet that has no access key, effectively removing these tokens from the outstanding token float.



Source: Coin Metrics, 5/1/22.

7 "Monetary Policy." EthHub. Accessed April 12, 2022. https://docs.ethhub.io/ethereum-basics/monetary-policy/.

In many ways, Ethereum's issuance schedule can be viewed similar to that of a corporation's share issuance and repurchasing strategy. It is generally accepted that repurchasing shares at certain times can reduce outstanding share count and help grow shareholder value. Similarly, issuing shares when a corporation needs capital may also make sense. This analogy is not without faults, as ETH issuance is intended to increase the security incentives for the network, rather than fund Ethereum or its developers in the way that corporate share issuance provides funding for public companies, but it does help illustrate how Ethereum's issuance of its own native token is intended to work. The network aims to issue the minimum amount of ether possible to maintain network security just as corporations issue and retire shares to try to maximize capital allocation decisions.

The recently added burning feature also reduces supply, and if continued over time, would likely provide a natural price catalyst assuming it is combined with continued demand for the network. Similar to most corporate share programs, Ethereum's future supply schedule is unknown but is intended to be altered in what is deemed to be in the best interest of the network. Whether "the network" is defined as the average platform user or ETH token holder is an important discussion mentioned later in the risks section of this report.

Non-Native (non-ETH) Tokens

There are other tokens besides ETH on the Ethereum network. Unlike bitcoin, Ethereum easily allows for non-native tokens to exist on its network rails. These non-ETH tokens can be either fungible, meaning they can be exchanged for other tokens, or non-fungible tokens (NFT).[8] Fungible tokens, also known as ERC-20 tokens, are often used in the funding and development of decentralized applications on the Ethereum network.

Non-fungible tokens, an emerging trend in digital assets these days, represent unique assets that are not interchangeable and for which true ownership is represented on the blockchain. These tokens represent some of the biggest use cases for the Ethereum network, and consequently, the ether token.

A Multipurpose Platform

Putting it all together, the combination of the Ethereum blockchain, its native ETH token, non-native tokens, and smart contracts, make for a multipurpose platform which allows developers to mold applications for their desired use case. This is why many refer to the Ethereum network as a "world distributed computer." In the Ethereum whitepaper, Vitalik Buterin described how these pieces all come

8 "Non-Fungible Tokens (NFT)." ethereum.org. Accessed April 12, 2022. https://ethereum.org/en/nft/.

together and what it creates:

> *"Ethereum does this by building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions."*[9]

We think the following visual helps illustrate how to think about the various functions and parts of the Ethereum network, and how they build on top of each other.

The core value proposition for ether grows as the number of tokens, smart contracts, and developers choosing to interact with the Ethereum network increases.

Ethereum and Bitcoin – How Do They Compare?

Because Ethereum leverages the core blockchain technology that Bitcoin revealed to the world and then adds additional functionality to it, the temptation may be to assume Ethereum is therefore a "better" or an improved version of Bitcoin. We do not believe either network can be deemed as "better" than the other for a number of reasons that we have detailed before[10] and will detail more reasons in this paper. In fact, the co-creator of Ethereum, Vitalik Buterin, noted in the Ethereum whitepaper:

9 Buterin, Vitalik. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." ethreum.org. ethereum.org, 2014. https://ethereum.org/en/whitepaper/#ethereum.

10 See "Bitcoin First" pages 12-15 for our discussion of bitcoin alternatives
Kuiper, Chris, and Jack Neureuter. Rep. *Fidelity Digital Assets / Bitcoin First*. Fidelity Digital Assets, January 31, 2022. https://www.fidelitydigitalassets.com/articles/bitcoin-first.

> *"The intent of Ethereum is to create an alternative protocol for building decentralized applications, providing a different set of tradeoffs that we believe will be very useful for a large class of decentralized applications,..."*[11]

We, like Buterin in the original whitepaper, also view Ethereum as an *alternative* protocol for building decentralized applications, which necessarily produces different tradeoffs, while the Bitcoin network remains potentially the best *monetary network* among the digital asset ecosystem in our opinion.

Ethereum's programming language is what is known as "Turing complete" whose main feature is the ability to program loops; not only does this increase functionality but it also means a program on a Turing-complete machine will always run to completion given enough time and resources. This is why Ethereum uses gas fees, a kind of metering device to incentivize code to be written economically and so programs do not get caught up in infinite loops, using up network resources indefinitely.

Bitcoin's programming language is Turing *in*complete. While this may sound like a deficiency, it is by design so that the network cannot get stuck in an infinite loop. It is actually more difficult to make sure a programming language is Turing incomplete, as a Turing complete language can be accidentally created. The takeaway is to emphasize that a user would want a relatively simple program to handle a monetary good, and one that emphasizes security and reliability, while someone who wants to build more functionality would require a more complex programming language.

The chart below summarizes some more of the differences between the Bitcoin and Ethereum networks, which we will expand upon later.

	Bitcoin Network	Ethereum Network
Primary Purpose	Most decentralized and secure monetary network	Distributed world computer, a multipurpose platform
Founder(s)	Unknown	Known
Speed of improvement implementation	Very slow and deliberate	Faster and more responsive to user demand
Programmable or Smart Contracts?	No (or very limited)	Yes
Ability to host multiple tokens?	No, only bitcoin	Yes
Monetary or Token Issuance Policy	Fixed, pre-programmed and has never changed	Has changed and is expected to change again
Auditability (How many tokens exist?)	Yes, very easy to audit at any time (can be done with consumer-grade computer)	Can be audited but may be more difficult
Level of Centralization	More decentralized	More centralized
Cost of node (a computer that maintains the ledger)	Cheap (~$100 per node)	Expensive (~$1,100 per node)
Consensus mechanism	Proof-of-Work	Currently proof-of-work; plans underway to move to proof-of-stake
Initial Funding	None (all tokens have been mined through proof-of-work)	Crowdsourcing and "pre-mined" tokens

11 Buterin, Vitalik. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." ethereum.org. ethereum.org, 2014. https://ethereum.org/en/whitepaper/.

The Ethereum Timeline – Past, Present, and Future

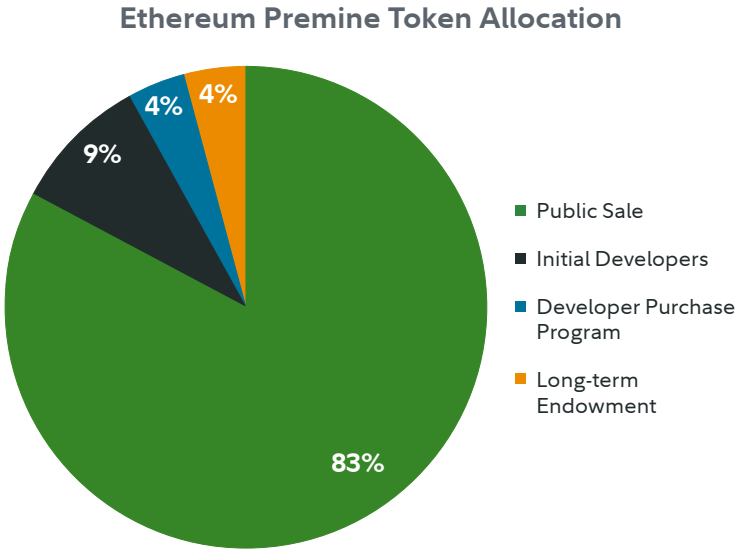
The Beginning and Founding of Ethereum

Ethereum's main founder, Vitalik Buterin, conceived the idea in 2013 and published the project's initial whitepaper in November of that year.[12] A number of individuals have become known as co-founders of the Ethereum network alongside Vitalik, including Gavin Wood, Charles Hoskinson, Anthony Di Lorio and Joseph Lubin.[13] The ideas behind Ethereum are best conveyed by Vitalik himself within the conclusion of the whitepaper stating,

> *"The Ethereum protocol provides for a platform with unique potential; rather than being a closed-ended, single-purpose protocol intended for a specific array of applications in data storage, gambling or finance, Ethereum is open-ended by design, and we believe that it is extremely well-suited to serving as a foundational layer for a very large number of both financial and non-financial protocols in the years to come."*[14]

In 2014, the group launched a campaign to raise funds in order to finance the building of this stated vision, ultimately raising over $18 million dollars in exchange for 60 of the initial 72 million ether (ETH) minted.[15] This put the initial sale price of ether at around $0.30 per ETH. The remaining 12 million ETH were split among the Ethereum Foundation, a non-profit organization dedicated to supporting Ethereum and its ecosystem, and Ethereum developers.[16]

This token launch method, whereby native tokens are created and distributed prior to the protocols launch, often in an effort to fund early developers



12 Buterin, Vitalik. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." ethereum.org. ethereum.org, 2014. https://ethereum.org/en/history/#whitepaper.

13 Hamacher, Andriana. "Who are Ethereum's co-founders and where are they now?" Decrypt, July 28, 2020. https://decrypt.co/36641/who-are-ethereums-co-founders-and-where-are-they-now

14 Buterin, Vitalik. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." ethereum.org. ethereum.org, 2014. https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_White_Paper_-_Buterin_2014.pdf.

15 Buterin, Vitalik. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." ethereum.org. ethereum.org, 2014. https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_White_Paper_-_Buterin_2014.pdf.

16 "History and Network Upgrades." EthHub. Accessed April 12, 2022. https://docs.ethhub.io/ethereum-basics/history-and-forks/.

and the protocol itself as well as gain community network effects, is known as pre-mining. The remaining 12 million token allocation resulted in 3 million ETH being placed in a long-term protocol endowment, 6 million Ether shared among 85 of the initial developers, and 3 million as a "developer purchase program" that gave Ethereum developers the ability to purchase Ether at crowdsale prices.[17] The Ethereum proof-of-concept, named Olympic, was released in May of 2015[18] and the Ethereum network went live in the months following (first live version was known as "Frontier").[19]

A History of Major Ethereum Network Upgrades

Name	Date
Frontier	07/30/2015
Frontier Thawing	09/07/2015
Homestead	03/14/2016
DAO Fork	07/20/2016
Tangerine Whistle	10/18/2016
Spurious Dragon	11/22/2016
Byzantium	10/16/2017
Constantinople	02/28/2019
Istanbul	12/06/2019
Muir Glacier	01/02/2020
London	08/05/2021

In line with Ethereum's complexity tradeoffs mentioned previously, the community has also shown little fear of change. The protocol has experienced major upgrades over 10 times throughout its history, many of which were done via "hard forking" the network – an alteration to the network's protocol that is not backwards compatible and requires users to upgrade their software.

The DAO Hack

In April of 2016, a decentralized autonomous organization (which is something we will detail below under "Current Ethereum Applications") known as "The DAO" raised funds for its initial token sale and received plenty of recognition for its large fund raising and innovative approach to restructuring traditional corporate business models. Unfortunately, The DAO was exploited through a security vulnerability in June of that year. Approximately 3.6 of the 11 million ETH raised by the group, worth over $50 million at the time, were moved into an address which required a 28-day holding period per the terms of the Ethereum smart contract.[20]

This created a divide within the Ethereum community, with some members advocating that code is representative of the common consensus of truth and funds taken due to a code vulnerability are rightfully owned by the hacker. Others were concerned with the size of the hack and felt that it was unethical, and the community should do what is necessary to return the funds to their "rightful" owner. The eventual outcome was a hard fork of the network creating two chains, a legacy chain which kept the hacked funds in place as

17 "Crypto Research, Data, and Tools." Messari Crypto News. Accessed April 12, 2022. https://messari.io/asset/ethereum/profile/launch-and-initial-token-distribution.

18 Buterin, Vitalik. "Olympic: Frontier Pre-Release." Web log. *Ethereum.org* (blog). Ethereum Foundation, May 9, 2015. https://blog.ethereum.org/2015/05/09/olympic-frontier-pre-release/.

19 "History and Forks of Ethereum." ethereum.org. Accessed April 12, 2022. https://ethereum.org/en/history/#frontier.

20 Siegel, David. "Understanding The DAO Attack." *CoinDesk*. Digital Currency Group, June 25, 2016. https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/.

the code had executed, now called Ethereum Classic, and the other, the Ethereum network we know today, which opted to overrule the exploit and return the funds to The DAO.[21]

Did the DAO Hack Illustrate Major Centralization Risks or Merely Early-Stage Hiccups?

This controversy highlights a few important things. First, in these early days Ethereum represented a more centralized project in which developers exhibited more influence over the trajectory and success of the network. One could argue that Ethereum was still in its infancy and allowing these stolen funds to remain in the hands of the hacker could have been seen as a critical blow to the community's confidence in the overall project.

Though it is less often cited, Bitcoin had a bug and blockchain rollback of its own in its infancy. In 2010, 184-billion bitcoin were minted as the result of an exploit which would later be thwarted and rolled back via a soft fork by developers Satoshi Nakamoto and Gavin Andresen.[22] All projects aiming for decentralization must begin with a relatively centralized beginning, even Bitcoin. While certain design tradeoffs may dictate one project's limitations to decentralization when compared to another, such as the case between Bitcoin and Ethereum, nearly all successful projects are able to become increasingly decentralized through time and adoption.

The ICO Craze of 2017

By the Fall of 2015, the first initial coin offerings on the Ethereum network took place and non-Ether tokens began to exist within the Ethereum ecosystem via the ERC-20 standard. Tokens could raise funds in a similar fashion to the Ethereum foundation, allocating their developers and treasury a portion of the network's assets. This would later lead to numerous project launches and culminated in the initial coin offering (ICO) craze of 2017 in which many projects were created with no viable use case outside of enriching project developers and insiders. One study found only 8% of ICOs issued in 2018 and the first half of 2019 traded above their initial price after six months.[23] ICOs still take place today, but the lessons from 2017 have led to some level of increased scrutiny surrounding initial token allocations (including the increased crackdown by regulatory agencies such as the SEC[24]), developer incentives, and overall project tokenomics.

21 Buterin, Vitalik. "Hard Fork Completed." Web log. *Ethereum.org* (blog). Ethereum Foundation, July 20, 2016. https://blog.ethereum.org/2016/07/20/hard-fork-completed/.

22 Stevens, Robert. "The Day Someone Created 184 Billion Bitcoin." *Decrypt*. Decrypt, August 26, 2020. https://decrypt.co/39750/184-billion-bitcoin-anonymous-creator.

23 Fromberger, Mathias and Haffke, Lars, *ICO Market Report 2018/2019 – Performance Analysis of 2018's Initial Coin Offerings* (December 31, 2019). Available at SSRN: http://dx.doi.org/10.2139/ssrn.3512125

24 "SEC Halts Alleged $1.7 Billion Unregistered Digital Token Offering." *Sec.gov*. U.S. Securities and Exchange Commission, October 11, 2019. United States Federal Government. https://www.sec.gov/news/press-release/2019-212.

The Road Ahead – Transitions and Upgrades

Today, much of the development roadmap surrounding Ethereum is focused on two key items – a transition to proof-of-stake (described below) and protocol scaling, both of which are core components to Ethereum's stated transition to "Ethereum 2.0" or "ETH 2.0." (Although we note the Ethereum Foundation has advocated to drop the term "ETH 2.0" and refer to it as simply Ethereum or Ethereum upgrades.)[25]

Proof of Stake (PoS)

To date, Ethereum has utilized a proof-of-work based consensus mechanism that is similar, but not identical, to that of bitcoin. However, the protocol developers of Ethereum have long planned for a transition to a proof-of-stake consensus mechanism.[26] It is important to note that the switch between proof-of-work and proof-of-stake is unrelated to transaction speed, capacity or throughput, but rather simply a matter of how the network chooses to order and validate incoming transactions.

Proof-of-work requires specialized equipment and an electricity input as well as a subsequent competition amongst miners to compete to mine each new block, and therefore validate a new batch of transactions. Similarly, proof-of-stake features a method for validating new transactions into blocks, but it does so via a wealth staking mechanism. In this system, instead of expending electricity and computing power that can be lost if a user does not follow the rules or acts maliciously, users lock up their tokens or wealth, which is then subject to being lost (or "slashed") if they do not follow the rules. Upon a successful transition to proof-of-stake, Ethereum users would be able to stake their Ether tokens to help secure the network while earning a yield for their efforts. Under proof-of-stake, miners are replaced with these staking validators and competition for each block is replaced with randomness via an algorithm.[27]

Proof-of-work is often criticized for its energy intensive nature, though this can also be looked at as a feature rather than a bug. The reliance on mining consensus, rather than staking validation, ensures that wealth is relatively less correlated to dictating what the protocol considers to be "truth." Instead of staking tokens that are native to that protocol, specialized mining equipment is required to validate new transactions. User rights within a proof-of-work protocol are virtually identical irrespective of whether they hold a large or small amount of the network's native token.

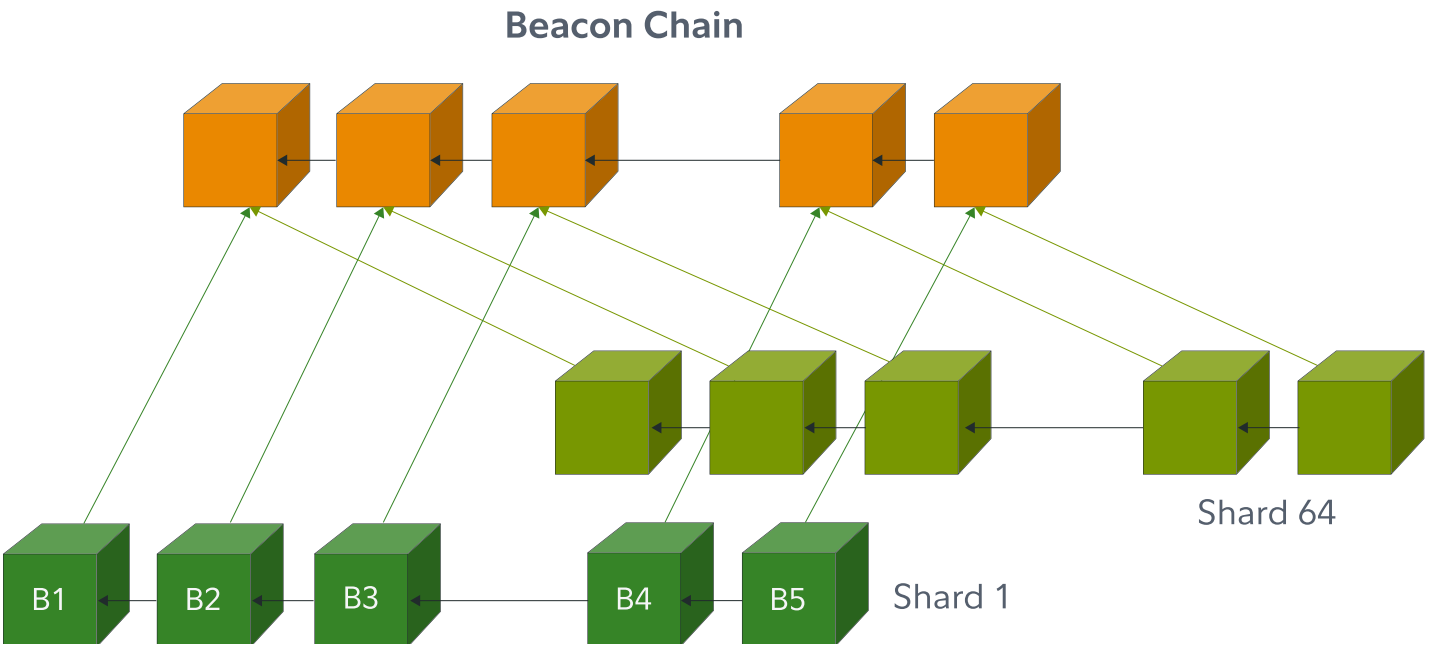
Under a proof-of-stake mechanism, this is not necessarily the case, as wealthier stakers technically do have more power over consensus. However, the combination of randomness and incentives to act in good faith help to remove some of these concerns. Proof-of-stake was introduced in a test-like environment in

25 "The Great Renaming: What Happened to Eth2?" *Ethereum.org* (blog). Ethereum Foundation, January 24, 2022. https://blog.ethereum.org/2022/01/24/the-great-eth2-renaming/.

26 "Proof-of-Stake (POS)." ethereum.org. Accessed April 12, 2022. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

27 "Proof-of-Stake (POS)." ethereum.org. Accessed April 12, 2022. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

December of 2020 with the introduction of the Beacon Chain, though the network still relies on proof-of-work today. This Beacon Chain is expected to become the proof-of-stake based consensus layer of the Ethereum network at some point in the future.[28]



Scaling

The other major, and arguably more important, upgrade that will be featured as part of the ETH 2.0 roll out is "sharding." This is an attempted scaling improvement by which the Ethereum database will be split into "shards," which are simply smaller individual chains, to reduce network congestion and increase transaction per second throughput. The implementation of shard chains is expected to take place in 2023[29] and would ideally help lower transaction fees on the network, a major issue that has caused users and developers to flock to other blockchains that are often more scalable, but at the cost of centralization. These individual shards, of which 64 are planned, will then rollup to the one master Beacon Chain.

In the meantime, Ethereum has become increasingly reliant on layer 2 rollup solutions that can help ease the burden associated with transaction congestion by bundling, or "rolling-up", individual transactions off-chain before settling them on the Ethereum base layer.[30] These layer 2 solutions are important in helping reduce network congestion, and therefore transaction fees, and will be an important piece of infrastructure for the ecosystem even after the planned scaling improvements associated with the ETH 2.0 roll out.

28 "The Beacon Chain." ethereum.org. Accessed April 12, 2022. https://ethereum.org/en/upgrades/beacon-chain/.

29 "Shard Chains." ethereum.org. Accessed April 12, 2022. https://ethereum.org/en/upgrades/shard-chains/.

30 "Scaling." ethereum.org. Accessed April 12, 2022. https://ethereum.org/en/developers/docs/scaling/.

Ethereum's Value Proposition

Current Ethereum Applications

Given the Ethereum network was the first to enable decentralized applications or dApps, many of the most popular dApps continue to run on the Ethereum network:

Top dApps by Balance ($USD Equivalent lock or on platform)

	dApp	Category / Use	Blockchain	Balance ($USD)
1	ETH2 Deposit Contract	DeFi	Ethereum	$26.34 B
2	Polygon POS Bridge	DeFi	Ethereum	$4.84 B
3	Uniswap V2	Exchange	Ethereum	$4.26 B
4	Curve	DeFi	Ethereum (and Others)	$4.25 B
5	ApeSwap	DeFi	BNB and Polygon	$4.08 B
6	Oasis App	DeFi	Ethereum	$3.15 B
7	Uniswap V3	Exchange	Ethereum	$2.9 B
8	Compound	DeFi	Ethereum	$2.41 B
9	AutoShark Finance	DeFi	BNB and Polygon	$1.68 B
10	Arbitrum	Other	Ethereum	$1.6 B

Source: dappradar.com as of 5/17/22.

While there has been an explosion in dApps with all kinds of use cases, there are a few main categories that the most popular dApps fall under, which we detail below. However, much like the internet, we would caveat this and note that there will likely be entirely new application categories within the next few years.

Decentralized Finance (DeFi)

The first, and arguably still most popular, decentralized finance applications replicated many of the traditional finance functions such as payments, lending, borrowing, saving, trading, and even insurance. However, given the programmability of smart contracts and how different things can be built upon each other, there has also been the emergence of new financial services that can only be done through decentralized applications. Therefore, "DeFi" has come to represent a kind of catch-all for anything that is financial-related but done on a blockchain and through decentralized applications.

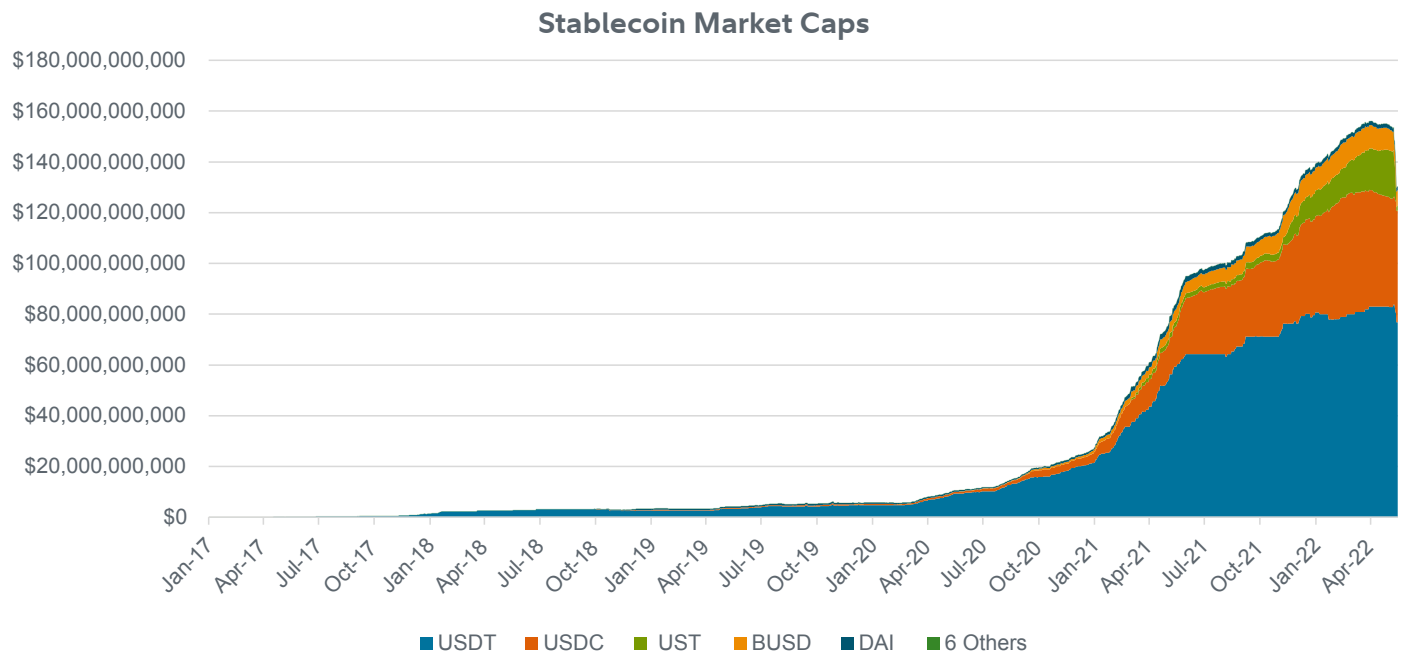
A comparison of traditional finance to DeFi can help illustrate some of the value proposition for DeFi:

Traditional Finance or "TradFi"	Decentralized Finance or "DeFi"
May be closed to customers due to geography, lack of identity verification, or credit metrics	Open to anyone with an internet connection
Trust in central authority or intermediary such as a bank	Decentralized, no single intermediary to trust (but you do need to trust the protocol or code)
High transaction friction - can have high costs or transactions can take days	Usually lower costs, transactions usually happen in minutes to a few hours
Low transparency (e.g. do not know exactly how loans are approved)	High transparency, most code is open-source and auditable and verifiable
Funds are held by intermediaries	Ability to control funds directly
Ability to censor (e.g. freeze accounts, block transactions)	Censorship-resistant
All activity linked to real identity	Pseudonymous
Limited hours that institutions are open	Always open and running

One example of a basic, but still powerful use of DeFi is borrowing and lending. Users who hold assets such as ether can lock them into a smart contract as a saver or lender, while the protocol facilitates the borrowing of those assets for a specific time period, automatically paying interest to the lender. What makes this different from a traditional borrowing/lending arrangement is that there is no bank or intermediary, no personal information needed, and everything is executed automatically through code.

Stablecoins

The Ethereum network also allows for the creation of stablecoins, which are tokens that are pegged to a popular fiat currency, such as the U.S. dollar. The value proposition is a digital asset that acts like a traditional currency, or in other words has little to no volatility when compared to something like the U.S. dollar. Since buying or selling digital assets like ether with U.S. dollars requires an "on-ramp," usually in the form of a regulated exchange, as well as high fees, the ability to swap between ether and a U.S. dollar-like token is very appealing for many users, especially those conducting DeFi transactions or perhaps doing a lot of trading. It is beyond the scope of this paper to delve into all of the uses of stablecoins, but suffice it to say these have become very popular, growing from less than $6 billion in total value at the end of 2019 to over $180 billion as of the middle of March 2022. We also note that at this time most stablecoins are fiat-backed by a central issuer, so while they are used in decentralized applications, they are ultimately tied to a central institution and therefore carry the related risks.



Source: Coin Metrics & Messari, 5/16/22. Updated through the 16th as UST is virtually non-existent.

Non-Fungible Tokens (NFTs)

As previously noted, the Ethereum network can host more than just ether tokens. While there are many non-ether tokens that are fungible like ether, there is also another class of non-ether tokens known as non-fungible tokens or NFTs. These are tokens that are digitally unique; no two NFTs are the same and each NFT has an owner. These tokens also live on the Ethereum network andtherefore their ownership can be verified and tracked.[31]

Factoid

In March 2021, Christie's Auction House sold an NFT for $69 million.[33]

NFTs can introduce scarcity and authenticity to things like digital art and music. While it was previously possible to buy and sell an original physical painting, it is now possible to do so with a digital piece of art. It is also easy to authenticate an NFT as genuine and prove its provenance.[32]

NFTs can also be linked to real-world (or non-digital) assets like real estate, enabling the "tokenization" of these assets. However, there is still the necessity for a link between the ownership mechanism of the real asset and the token, such as a way to link the deed to a piece of property to a token.

31 "Non-Fungible Tokens (NFT)." ethereum.org. Accessed April 12, 2022. https://ethereum.org/en/nft/.

32 For more on NFTs and the potential value creation, see Harvard Business Review. "How NFTs Create Value"by Steve Kaczynski, Scott Duke Kominers. *Harvard Business Review*, (November 10, 2021). https://hbr.org/2021/11/how-nfts-create-value.

33 Beeple. *EVERYDAYS: THE FIRST 5000 DAYS. Christie's*. Christie's, February 16, 2021. https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924.

Decentralized Autonomous Organizations (DAOs)

Smart contracts and programmability have also enabled a new kind of entity known as a decentralized autonomous organization or DAO. This is an organization that adheres to rules programmed into its code that are then maintained and executed on the blockchain. While the smart contracts are autonomous and therefore execute the agreed upon decision and conditions, a DAO is ultimately owned and governed by its members. Proposals for the DAO to do something or change its code are put forth by members and then voted on.

DAOs may offer a new way for people to organize and conduct business or complete a specific mission or task. Compared to corporate or other traditional organizational structures, DAOs are very democratic, with voting needed to make changes or decisions. Services are handled automatically (such as distribution of funds) and everything is verifiable and transparent.[34]

Example of Constitution DAO

One example of a recent DAO is "Constitution DAO" that was formed in November 2021 with the express purpose of purchasing a copy of the United States Constitution that was going up for auction.[35] The DAO raised approximately $47 million in ether, and although the DAO ultimately lost the auction to a higher bid, the event demonstrates some interesting points. First, how quickly thousands of people were able to efficiently pool their money together for a cause, especially when typical auctions are won by only one wealthy individual. Participants were able to do this without having to trust one person or company with their funds, and then automatically receive their funds back after the bid failed.

But How Does Value Accrue to Ether?

The Ethereum network's intended transition to proof of stake does alter some of the tokenomics and considerations for investment in the ETH token itself. Today, ETH's single true use case is to function as the native currency for transactions on the Ethereum blockchain, however, this becomes dramatically altered upon a successful transition to proof of stake. Once changed, ETH will become a vital part of the network's security and transform into a yield-bearing asset. ETH then offers the ability to function in a similar capacity to application specific miners on a proof-of-work blockchain, only these ETH "miners" are non-depreciating and can be used or traded along the network. Similarly, ETH as a consensus validating asset means that overall network usage and the importance of maintaining adequate security will be a potential driving force for future price appreciation of the asset.

34 "Decentralized Autonomous Organizations (DAOs)." ethereum.org. Accessed April 12, 2022. https://ethereum.org/en/dao/.

35 Patel, Nilay. "From a Meme to $47 Million: Constitutiondao, Crypto, and the Future of Crowdfunding." *The Verge*. Vox Media, LLC, December 7, 2021. https://www.theverge.com/22820563/constitution-meme-47-million-crypto-crowdfunding-blockchain-ethereum-constitution.

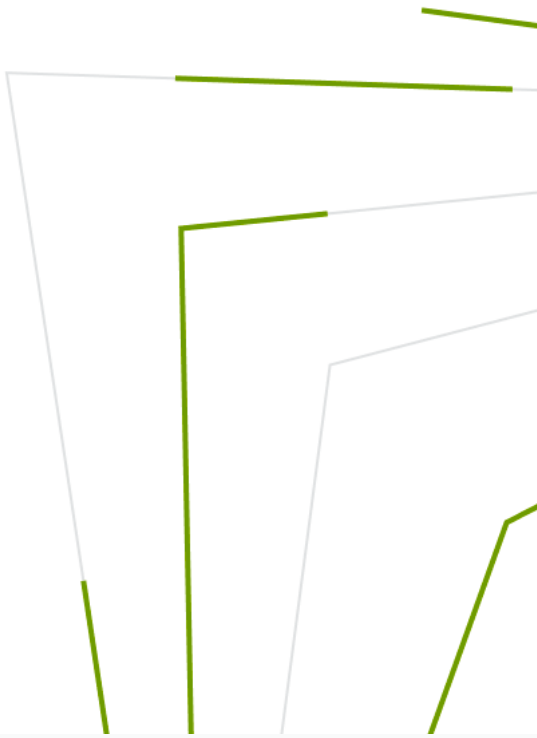
Risks

The investment thesis for any asset wouldn't be complete without considering the risks involved. Ethereum has come a long way in its development, but even today the network is still far from what many would consider its fully matured form. The many tradeoffs and upgrades that the platform has opted to make carry both potential rewards and risks to the value of the network.

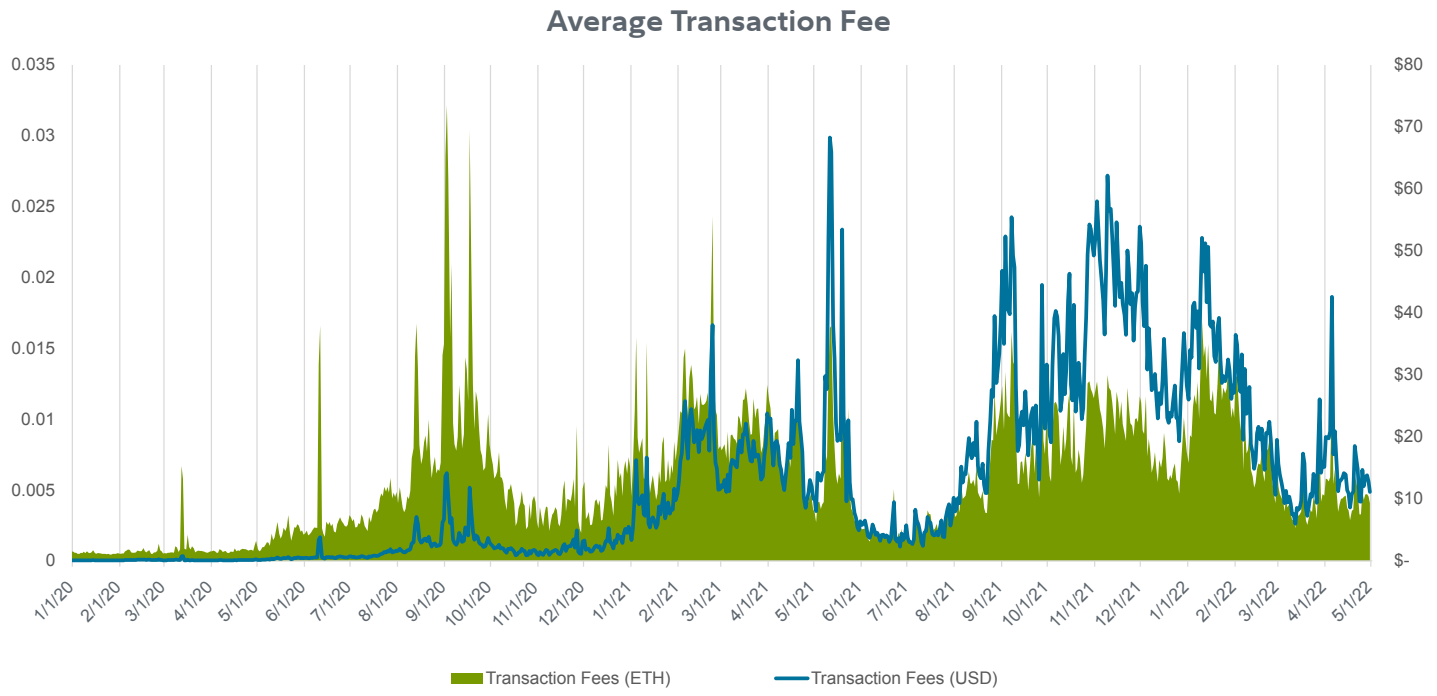
> We have chosen to highlight a few of the major categories of risks associated with Ethereum below. Individuals considering an investment in ETH should be sure to do their own due diligence and carefully consider the potential risks beyond just what is listed below.

Explicit Tradeoffs Made for Scalability

Ethereum's success has resulted in a clear increase in competition, particularly in recent years. Network congestion has been an issue as the number of developers, applications, and users continue to grow. This increased use of the Ethereum network has caused large spikes in transaction fees for prolonged periods of time. Even moments that are generally accepted as being low volume and cheap often still result in transaction fees well in excess of $10. Vitalik Buterin himself has been quoted as saying the following about Bitcoin, "the internet of money should not cost 5 cents per transaction,"[36] yet the Ethereum platform has yet to make meaningful progress towards these price levels when interacting with the majority of its popular applications.



36 Crypto Me! "'The Internet of Money Should Not Cost 5 Cents per Transaction." -Vitalik Buterin." YouTube. YouTube, December 9, 2017. https://youtu.be/unMnAVAGIp0.



Source: Coin Metrics, 5/01/22.

This concern is something that the Ethereum community is actively working on. As mentioned earlier, scaling is one of the primary goals associated with the transition to ETH 2.0. Additionally, "layer two networks", mentioned previously, have been successful in offering alternative ways to utilize the Ethereum blockchain. This is one of the most important challenges that the Ethereum network must continue to aim to overcome, as other platforms have shown varying levels of success when continuing to trade off centralization for greater speed and lower costs.

Changing Token Issuance Policy

The narrative that Ethereum's token issuance policy is "ultrasound", claimed by some in the community,[37] may feel off-base seeing that Ethereum's token supply is fluid and subject to change in the future. Today, it appears the issuance rate of the network will likely continue to fall while the newly introduced burning mechanism should continue to, at times, create a net reduction in supply, ultimately a deflationary effect. However, similar to the corporate share program analog we outlined earlier, this is surely a policy that could be altered in one direction or the other if warranted by the network and community.

Another concern that is important to raise is whether these alterations to Ethereum's issuance policy have been in the best interest of the network as a whole. The burning of ETH reduces the total reward that would otherwise have been given to miners, and in the future staking validators, opting to reduce token supply at the expense of would-be security incentives. This burning raises the relative percentage

37 Quarmby, Brian. "Ethereum Is Becoming Ultrasound Money, ConsenSys Founder Says." *Cointelegraph*. August 5, 2021. https://cointelegraph.com/news/ethereum-is-becoming-ultrasound-money-consensys-founder-says.

of ether owned by each token holder and is beneficial to ETH token holders. One could also argue that reducing the issuance subsidy, and burning portions of transaction fees, raises the costs to interact with the network. In this sense, reductions in mining subsidies, through reduced issuance or increased burning, may be viewed as a battle between asset holders and network users. This particularly effects the average user, as transaction fees are likely to be a larger relative portion of smaller transactions. This is certainly a consideration that the community seems likely to take into account when deciding upon future adjustments to Ethereum's monetary policy. It is one of the key reasons that we believe Ethereum's future monetary policy carries some uncertainty.

Transition to Proof-of-Stake Risks

Ethereum's planned transition to proof-of-stake also carries a host of potential dangers. Switching the governance mechanism with which transactions are batched and validated is a potentially risky proposition, as it represents an alteration to one of the networks core security processes. Although other networks exist in a proof-of-stake model, none have transitioned their consensus mechanism with the size, scale, and decentralization that Ethereum offers. Even upon successful transition, concerns will likely remain regarding centralization and the fact that wealth will then be used to dictate control over transaction validation. Ethereum 2.0 staking requires a minimum of 32 ETH to become a full validator,[38] which will likely cause many to utilize aggregator staking services and has the potential to create large staking honeypots that could raise concerns surrounding the possibility of groups being able to co-opt the networks consensus.

However, it is important to acknowledge that the new proof-of-stake chain, known as the Beacon Chain, has already launched (in parallel to the original blockchain) and allows for users to lock their funds in and stake until the full ETH 2.0 merge. Moreover, in regard to concerns surrounding centralization risks the Ethereum community states,

> *"The threat of a 51% attack still exists in proof-of-stake, but it's even more risky for the attackers. To do so, you'd need to control 51% of the staked ETH. Not only is this a lot of money, but it would probably cause ETH's value to drop. There's very little incentive to destroy the value of a currency you have a majority stake in. There are stronger incentives to keep the network secure and healthy...Stake slashings, ejections, and other penalties, coordinated by the beacon chain, will exist to prevent other acts of bad behavior. Validators will also be responsible for flagging these incidents."* [39]

38 "Ethereum Staking." ethereum.org, April 4, 2022. https://ethereum.org/en/staking/.

39 "Proof-of-Stake (POS)." ethereum.org, January 26, 2022. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

Centralization Risks

Critics of the Ethereum network, particularly those from the Bitcoin community, often point towards the centralization-scalability tradeoff as Ethereum's biggest flaw. After all, Ethereum's ability to allow for increasingly complex applications to be built on its network does come at a direct cost.

Much of this tradeoff results in a larger blockchain that requires more expensive equipment to adequately maintain the network's historical ledger. This leads node operators, those maintaining a copy of these historical transactions, to become more reliant on third-party hosting services. According to publicly available data, around 20% of Bitcoin nodes rely on third-party cloud services versus nearly 70% for Ethereum.[40] Furthermore, the specifics surrounding what is regarded as a sufficient historical ledger can lead to long debates about whether certain data is necessary to maintain a given blockchain's historical ledger and direct comparisons aren't always possible.

This concern does lend itself towards questions regarding the relative level of censorship resistance and decentralization that the Ethereum network offers. Something that is likely to continue to be worked on over time in conjunction with the sharding of the Ethereum chain – lowering the hardware requirements to maintain a certain portion of historical transactions.

Conclusion

It is undeniable that the Ethereum network opened a world of new possibilities by extending blockchain technology to include dramatically enhanced programmability and smart contracts. We believe we have only just begun to see some of the applications of this technology. However, we have seen, and believe we will continue to see, fierce competition between Ethereum and other smart contract blockchains. Whether Ethereum continues to grow in adoption, users, and developers, will depend on whether it can strike the right balance between various tradeoffs as well as if its current roadmap to transition to proof-of-stake and scaling solutions will be successful. An ambitious roadmap and continued development in applications and potential use cases should, at the very least, lead to an exciting ecosystem to continue watching mature.

40 "Bitcoin Network 24-Hour Charts." Bitnodes. Accessed April 12, 2022. https://bitnodes.io/dashboard/.
"Ethereum Mainnet Statistics." Accessed April 12, 2022. https://www.ethernodes.org/network-types?synced=1.

For institutional use only.

The information herein was prepared by Fidelity Digital Asset Services, LLC ("FDAS LLC") and Fidelity Digital Assets, Ltd ("FDA LTD"). It is for informational purposes only and is not intended to constitute a recommendation, investment advice of any kind, or an offer to buy or sell any asset. Perform your own research and consult a qualified advisor to see if digital assets are an appropriate investment option.

Digital assets are speculative and highly volatile, can become illiquid at any time, and are for investors with a high-risk tolerance. Investors in digital assets could lose the entire value of their investment. Digital assets may also be more susceptible to market manipulation than securities. Digital assets are not insured by the Federal Deposit Insurance Corporation or protected by the Securities Investor Protection Corporation.

Accounts for and custody and trading of digital assets are provided by Fidelity Digital Asset Services, LLC, which is chartered as a limited purpose trust company by the New York State Department of Financial Services to engage in virtual currency business (NMLS ID 1773897). FDA LTD relies on FDAS LLC for these services. FDA LTD is registered with the Financial Conduct Authority under the U.K.'s Money Laundering Regulations. The Financial Ombudsman Service and the Financial Services Compensation Scheme do not apply to the cryptoasset activities carried on by FDA LTD.

To the extent this communication constitutes a financial promotion in the U.K., it is issued only to, or directed only at, persons who are: (i) investment professionals within the meaning of Article 19 of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the "FPO"); (ii) high net worth companies and certain other entities falling within Article 49 of the FPO; and (iii) any other persons to whom it may lawfully be communicated.

This information is not intended for distribution to, or use by, anyone in any jurisdiction where such distribution would be contrary to local law or regulation. Persons accessing this information are required to inform themselves about and observe such restrictions.

FDAS LLC and FDA LTD do not provide tax, legal, investment, or accounting advice. This material is not intended to provide, and should not be relied on, for tax, legal, or accounting advice. Tax laws and regulations are complex and subject to change. You should consult your own tax, legal, and accounting advisors before engaging in any transaction.

This material may be distributed by the following entities, none of whom offer direct exposure, clearing or custody for digital assets: Fidelity Distributors Company LLC ("FDC"), National Financial Services LLC ("NFS"), or Fidelity Brokerage Services LLC ("FBS"). FDC, NFS, and FBS, and their representatives, may have a conflict of interest in the products or services mentioned in these materials because they have a financial interest in them, and receive compensation, directly or indirectly, in connection with the management, distribution, and/or servicing of these products or services.

Fidelity Digital Assets does not assume any duty to update any of this information.

1024435.3.0