GLOBAL X ETFs RESEARCH

Ethereum: The Basics

Authored by:

Digital Assets Team
Global X Research

Date: March 10, 2022
Topic: Digital Assets

Editor's Note: We included a glossary for all terms highlighted in **sea green**.

Bitcoin's creation in 2009 marked the first successful application of **blockchain** technology as a finite-supply decentralized currency. Significantly, it was open to anyone. Bitcoin inspired developers to discover broader tools and applications powered by the security, transparency, and scalability of blockchain technology. While the Bitcoin network provided a base for a medium of exchange, a young programmer saw it as a method capable of challenging centralized entities across the economy.

In 2013, at just 19, Vitalik Buterin published the Ethereum whitepaper, in which he introduced a novel, general-purpose blockchain network that allows developers to build programable conditions and applications. In essence, Buterin created a system of programmable money that revolutionized how people think about, create, and deploy blockchain technology.

What to Know About Ethereum, Its Key Components, and How it Works

Because of its growing status and potential investment implications, this report answers basic questions about the Ethereum network.

- **What is Ethereum?** A decentralized blockchain with smart contract functionality.
- **What is Ether (ETH)?** The native currency of Ethereum.
- **What are nodes?** Computers running an Ethereum client to validate transactions and blocks.
- **How does mining work?** Special nodes solve a mathematical puzzle to create the chain's next block.
- **When does true settlement occur?** When a transaction has a sufficient number of confirmations.
- **What are smart contracts, and why are they important?** Programmable contracts based on pre-defined conditions.
- **What are decentralized applications (DApps), and why are they important?** Applications built using smart contracts.
- **What's ahead for the Ethereum network?** A transition to a consensus mechanism that can make the network more scalable and environmentally friendly.
- **Why is ETH valuable?** It dictates the network's economy.
- **Why Ethereum now?** The largest and most adopted smart contract blockchain offers value potential and growth.

Ethereum: A Blockchain with Smart Contract Functionality

Ethereum's launch in July 2015 introduced a novel blockchain with a built-in **Turing-complete language**, which is a programming language that can be used to embed logic and complete more advanced transactions than simple payments. The introduction of this language has allowed developers to create and integrate applications into Ethereum, serving as the base layer of an open ecosystem capable of hosting **smart contracts** and **decentralized applications (DApps)**.

Smart contracts comprise much of Ethereum's value proposition. A smart contract has predefined criteria that self-execute a response based on programmed conditions, and the agreement is recorded in the blockchain. Smart contracts eliminate the need for a third-party intermediary.

DApps are front-end and user-targeted applications created and deployed from smart contract programmability. These programable contracts are used to create **decentralized financial service applications (DeFi)** and **non-fungible tokens (NFTs)**, which represent the digital ownership of unique assets. Smart contracts are also used to create and coordinate decentralized governance entities called **decentralized autonomous organizations (DAOs)**. The universe of DApps within the network represents the Ethereum ecosystem.

The Ethereum network uses fully transparent blockchain technology to record **transactions** and track **states** on the ledger. Network participants can find a consensus state, which is where they agree on the blockchain's distributed ledger, by independently validating transactions and **blocks** against the protocol rules. Blocks are individual data structures built from an aggregate transaction list and include a reference to its parent, or previous, block.

The **Ethereum Virtual Machine (EVM)**, Ethereum's distributed state machine, is responsible for maintaining the network's data structure and standards. In essence, the EVM defines the rules for calculating a transition in state between blocks. A transition in state could be a simple change in an account balance, or it could be the result of a more complex smart contract interaction.

Ether (ETH): The Native Cryptocurrency That Powers the Ethereum Network

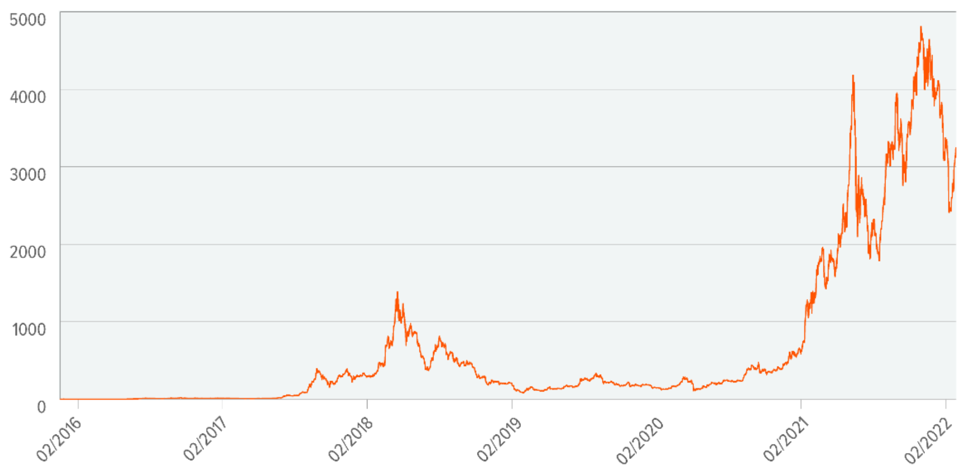
Ether (ETH) can be used to send simple payments, similar to bitcoin, but it is more akin to a commodity than a currency because it is primarily used to pay for decentralized computation on Ethereum. All transactions and smart contract deployment on Ethereum cost a variable fee to be paid in ETH. A simple payment is typically cheaper than a smart contract interaction. This payment scheme creates a natural demand for ETH, as Ethereum DApp end-users must purchase ETH to interact with the platform.

ETH has no physical representation; it is a digital bearer asset owned by whoever possesses the corresponding private key. Similar to Bitcoin, Ethereum uses **public-key cryptography** and **digital signatures** to prevent bad actors from spending someone else's ETH. For a deeper dive into public-key cryptography and digital signatures, see Bitcoin: The Basics.

ETH first went on sale on September 2, 2014, priced at 2,000 ETH per bitcoin (BTC). Currently, ETH is the second-largest cryptocurrency with a total market cap of $356 billion.[1]

ETHER (ETH) PRICE TODAY

Source: Etherscan.io as of March 1st, 2022

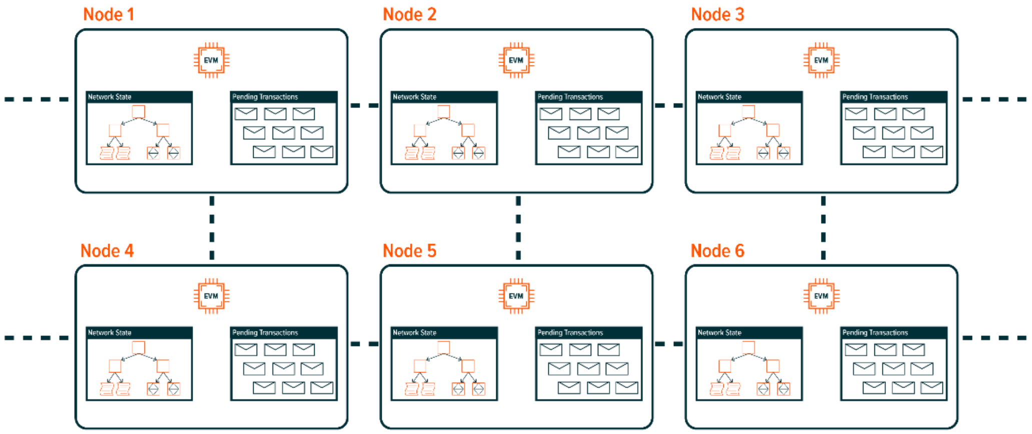


Nodes: The Computers Validating Transactions and Securing the Network

Nodes are the computers in the Ethereum network running an Ethereum client. An Ethereum client is the software that implements the Ethereum protocol, or the network's rules. The Ethereum network is an aggregation of connected nodes, each of which verifies that the transactions and blocks received are valid under the protocol rules before being added to the blockchain.

THE INTERCONNECTED NETWORK OF NODES

Source: Global X ETFs

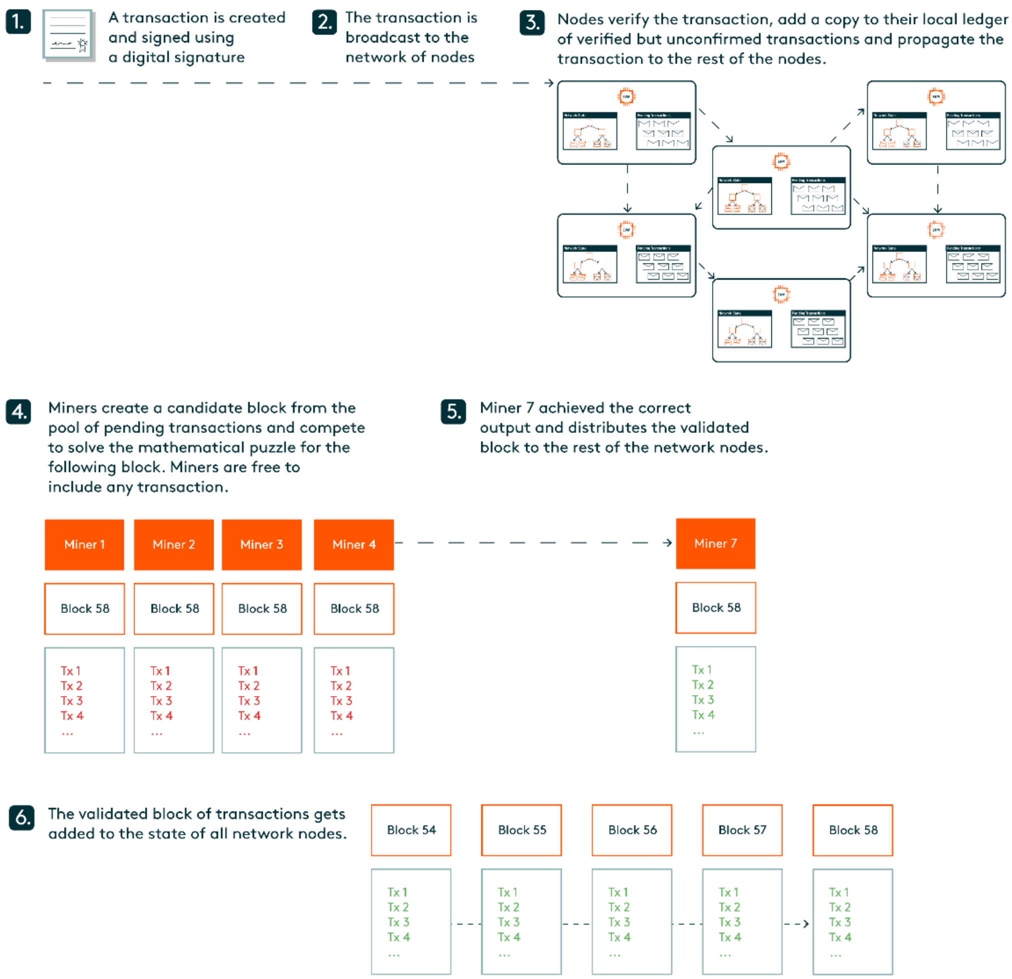


Transactions alter the state of data within the network, and they generally involve the transfer of digital assets or smart contract execution. All transactions must include an ETH-denominated transaction fee known as a **gas fee**, which represents the cost of publishing, validating, executing, and storing the transaction on the blockchain.

Once a transaction is digitally signed by a user's private key, it is broadcasted to the network of connected nodes. When a node receives a new transaction, the Ethereum client independently verifies the validity of this transaction against a comprehensive set of criteria outlined in the protocol rules, including an evaluation of the digital signature. If the transaction is valid, the node saves the transaction within its local pool of pending transactions and further propagates it to all of their neighbor nodes. This network of interconnected nodes makes it possible for transactions to be distributed, validated, and recorded by all participants in a matter of seconds.

LET'S WALK THROUGH AN ETHEREUM TRANSACTION

Source: Global X ETFs



Mining Nodes: Special Nodes that Solve a Mathematical Puzzle to Create the Next Block

All Ethereum nodes independently verify transactions, but **mining nodes**, the miners, are a special type that aggregate transactions into the blocks that are recorded onto the blockchain for settlement. In that sense, mining nodes are distinct because they create blocks of transactions on the chain.

Each node maintains a pool of verified but pending transactions known as the mempool. Transactions are removed from the mempool once a miner includes them in a mined block. Mining nodes dedicate large sums of computational resources in a competition to be the first to solve a challenging mathematical puzzle. The solution to the puzzle is known as a **Proof-of-Work**, the consensus mechanism that secures the integrity of the network.

The puzzle is solved by brute force computation, where miners iterate different inputs through a **cryptographic hash function** searching for a rare output, or **hash**. Ethereum relies on a different cryptographic hash function than bitcoin, and miners are not in direct competition with each other. The Proof-of-Work is difficult to find, but any node can trivially verify that the miner expended the computational resources to find the solution. In the same way that a transaction is considered valid only if it has a valid digital signature, a candidate block requires a Proof-of-Work to become a valid block. Achieving the particular output through Proof-of-Work ahead of all other participants allows a miner to validate, record, and propagate the candidate block.

Once a miner becomes the first participant to solve the mathematical puzzle of the next block, they broadcast the validated block through the network. Each node verifies the validity of the newly received block and then adds it to their copy of the blockchain. The receipt of a new valid block resets the mining game. All miners create a new candidate block of transactions and try to be the first to solve the puzzle for the next block to be included in the blockchain. The **block times**, which are typically between 12 and 14 seconds, dictate this constant flow of new blocks. Additionally, the **block size** is limited, and not all pending transactions are included in a block.

Miners are financially incentivized to be the first to solve this puzzle. The miner who first sends a new block with a valid Proof-of-Work can claim the 2 ETH **block reward** and a portion of the gas fees inside the block. Additionally, by setting the order of transactions in their blocks and due to **front running** tactics, miners can generate an incremental revenue stream known as **miner extractable value (MEV)**.

Gas fees in a block can be broken down into a base fee and a tip, both of which fluctuate in price with block space demand. The tip is paid directly to the miner as an incentive to prioritize the inclusion of a transaction in a block. The base fee resembles a share buyback, in that it is burned and the corresponding ETH is removed from the circulating supply.

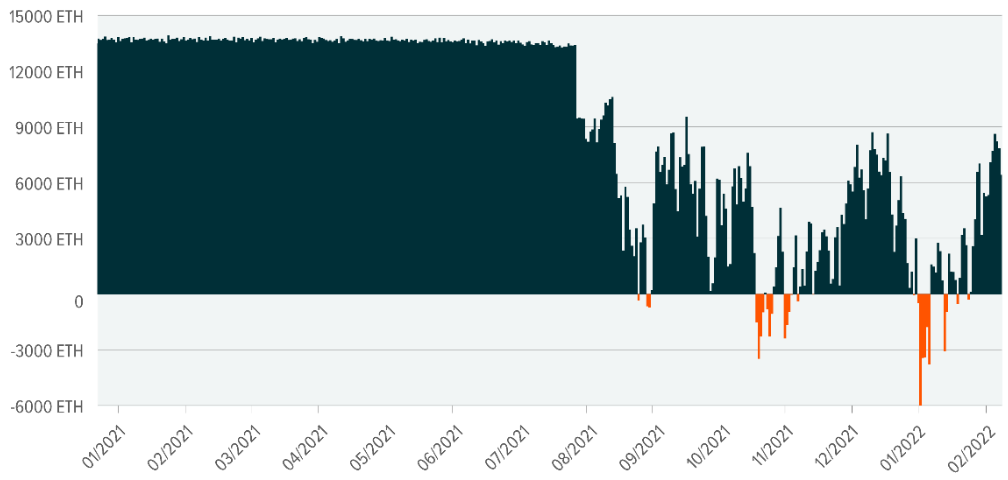
Ethereum Improvement Proposals (EIPs) are designed to incentivize network participants and builders to constantly improve the Ethereum network. One such proposal was this gas fee structure. Implemented in August 2021 through Ethereum Improvement Proposal 1559 (EIP-1559), it created a direct correlation between network usage and ETH issuance.

EIP-1559 creates value for ETH holders because the burning mechanism reduces the net supply issuance rate. As more transactions are conducted **on-chain**, more gas is burned, which has the potential to reduce or eliminate the impact of the new ETH supply created from block rewards. If network demand is high and the burning mechanism outweighs the new issuance from block rewards, ETH can become a deflationary asset. To date, more than 1.9 million ETH have been burned since the rollout of EIP-1559, reducing ETH's net issuance by more than 68%.[2]

The increased popularity of NFTs and the transaction volume they generate has created more demand for block space, increasing the amount of ETH being burned. NFT marketplace OpenSea has been the largest contributor to burned gas fees since the EIP-1559 rollout with a total of 230,041 ETH.[3]

THE BURN'S EFFECT ON THE ISSUANCE RATE SINCE INCEPTION

Source: Etherscan.io as of March 1st, 2022



True Settlement: When a Transaction Has a Sufficient Number of Confirmations

A transaction is often referred to as settled when it's included in a block. But because certain scenarios can cause the blockchain to fork temporarily and reorganize in the short term, certain conditions must be met for true settlement.

True settlement occurs after a sufficient number of **confirmations** are received, meaning blocks added to the chain on top of the block that includes a specific transaction. Given that blocks are linked together with each newly mined block referencing the prior block's hash, transactions become more secure and immutable as the number of blocks they're buried beneath increases. For context, popular centralized exchanges typically consider a transaction to be valid after 20 to 50 confirmations are recorded, which should only take a few minutes with Ethereum block times.

For a malicious actor to reverse a transaction, they would need to go back to the block that contains the transaction that they want to manipulate. So, if a transaction had 50 confirmations, they would need to go back 50 blocks. They would then need to re-mine that block and the other subsequent blocks on a **forked chain** and find a valid Proof-of-Work for each block. At the same time, all good actors following the protocol rules would be mining and extending the **main chain**, which is the chain with the most cumulative mining work on it.

To overcome this block deficit versus the main chain, the malicious actor would need to control more than 50% of the total network's computational power for a sufficient period of time. In addition, the malicious actor would face material risk because if they failed, they would waste their electricity without any ETH rewards.

Smart Contracts: The Programmable Infrastructure for DApps

Smart contracts offer the ability to script self-executing programs and agreements into Ethereum via specific programing languages that adhere to EVM standards. Developers can use a proprietary programing language Solidity, which was created to facilitate access to script tools for less-advanced participants. Developers can also use more advanced languages such as Vyper and Yul.

Said another way, smart contracts are programmatically executed contracts based on code. Data feeds, conditions, rules, and agreements embedded in the contract automatically trigger a pre-defined outcome without the need for a trusted intermediary to execute the contract. Any decentralized application can deploy a smart contract and compose functionality, such as supporting asset swaps or lending primitives.

Ethereum smart contracts are activated and deployed by submitting the contract as a transaction. They also have ETH balances that can trigger transactions through the network once the conditions of the contract are met. Because the network is open source, a library of implemented smart contracts is available for developers to reference, which enhances the composability of application development.

Smart contracts often incorporate real-world data feeds as input variables to determine a contract's output. Oracles are the entities that facilitate the connection and interoperability between blockchains and external systems. Oracles allow smart contracts to execute based on input data that is not natively available on the blockchain. Common examples include price data, weather data, election results, internet of things (IoT) sensor readings, ID verification for know your customer (KYC) standards, and verifiable random functions.

Because oracle-provided data can determine the output of many smart contracts, allowing a centralized entity to provide this information would defeat the purpose of using a trustless blockchain. Chainlink is a good example of a decentralized oracle network designed to solve this problem. It relies on a network of independent oracle nodes that are financially incentivized to deliver accurate real-world data on-chain in a trustless fashion.

DApps: Applications Built Using Smart Contracts

Smart contracts allow decentralized applications to create protocols with varied use cases and rules. DApps use the Ethereum blockchain for data storage and security, and they use smart contract technology for application logic. In essence, a DApp is just like an app with a user interface that's hosted on the web, but a smart contract that runs on a decentralized network of computers facilitates the DApp's backend computation.

This feature gives DApps resiliency because the execution of the code does not depend on a centralized cloud provider. The Ethereum network includes a range of DApps, including financial applications, governance structures, supply chain management projects, file storage, and non-fungible tokenization initiatives.

Decentralized financial services applications are prominent within the Ethereum DApp ecosystem. Some of these DeFi protocols feature native tokens, and many of the top DeFi apps comply with **ERC-20** standards. Popular **stablecoins** such as USDT, USDC, and DAI also use ERC-20 token standards. ERC-20 standards allow developers to build interoperable and **fungible tokens** under the same guidelines and compatibility framework, which creates optimal conditions for application and smart contract **composability**.

DeFi applications decentralize many traditional financial transactions, such as borrowing and lending, asset exchange, derivatives, insurance, and asset management. Two of the most popular applications today are Uniswap and Aave. Uniswap is a non-custodial, open-source, decentralized automated market maker that provides liquidity pools for buyers and sellers looking to exchange assets. Uniswap allows individuals to act as a market maker by depositing liquidity into trading pools, earning transaction fees from the users' trades against their liquidity. In January 2022, Uniswap liquidity pools traded approximately $58 billion in volume.[4] Aave is a decentralized, non-custodial liquidity and money marketplace for borrowing and lending digital assets. For example, a market participant can use Aave to get an instantaneous asset-backed loan on their digital assets.

Another popular smart contract application includes an alternative Ethereum token standard. **ERC-721** standardizes the creation of non-fungible tokens. NFTs are non-interchangeable tokens that cannot be replicated, meaning no two tokens are the same. To date, digital art is the predominant use case for NFTs. But given their broad potential scope, we expect more creative applications of NFTs to emerge in areas such as play-to-earn concepts in the gaming sector, real estate tokenization, ticketing, experiences, identity tags, exclusive access, memberships, and supply chain timestamps.

On-chain decentralized autonomous organizations (DAOs) also use Ethereum's blockchain infrastructure and smart contract technology for voting rights and decision-making. Popular use cases include DeFi DAOs, where participants can trade digital assets for governance tokens. Token holders can vote for asset allocation and investment decisions from the treasury of accumulated assets, and the rewards from such allocations can be paid out to the token holders.

What's Ahead for the Ethereum Network: Updates That Facilitate Scalability

Considering the growth of the Ethereum network, developers have agreed to a roadmap with several upgrades. These updates include a change in consensus mechanism in an attempt to make the network more scalable and environmentally friendly.

The Shift from Proof-of-Work to Proof-of-Stake

Previously referred to as Ethereum 2.0, the Ethereum Consensus Layer is Ethereum's upgraded roadmap that includes changes to the network as it shifts into its new state. This upgrade allows for better scalability with more modest hardware and energy needs.

Proof-of-Work provides strong security guarantees, but it requires significant hardware and energy. **Proof-of-Stake** requires minimal energy in comparison. **Validators** in a Proof-of-Stake consensus are analogous to miners in a Proof-of-Work consensus. Validators are responsible for ordering transactions, creating new blocks, and attesting to the blocks that other validators create.

Instead of using electricity to prevent network manipulation, Proof-of-Stake requires validators to post ETH as collateral to secure the network. When validators post their assets, they know that their assets will be seized if they act maliciously or fail to perform their responsibilities, a process known as **slashing**. The risk of slashing incentivizes validators to follow the protocol rules and act in the network's best interests. To become a validator, market participants must stake 32 ETH. Smaller market participants can participate in liquid staking pools through platforms like Lido, aggregating smaller amounts of ETH into 32-ETH increments and splitting the rewards accordingly.

Validators can be broken down into two categories: **proposers** and **attestors**. Proposers are chosen at random from the set of validators to propose the next block in the chain. Validators who are not chosen as proposers must attest to the proposal. Attestors review the proposed block and attest that it is valid under the protocol rules. For their participation, proposers and attestors are incentivized with ETH rewards. However, their staked assets are at risk if they act maliciously or fail to perform their responsibilities. Explicitly malicious behavior or deliberate collusion will result in a validator losing their entire stake. Less malicious acts, such as failing to validate due to a server outage, can result in only a small percentage of the stake being slashed.

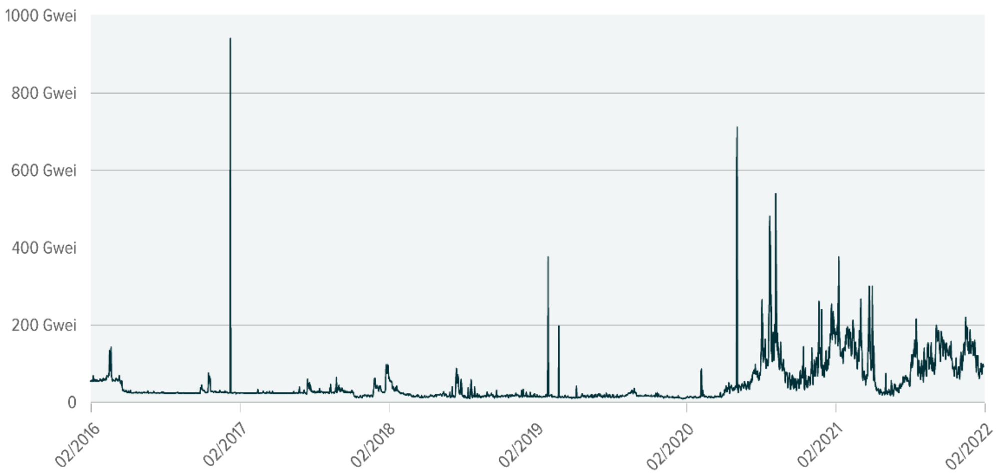
The Solutions Used to Scale Ethereum

The Ethereum network has hit capacity limitations due to its growing user base interacting with an increasing number of DApps. Greater demand for Ethereum limited block space has increased the volatility of gas prices in recent years and made the network prohibitively expensive for all but the largest market participants.

Ethereum gas fees are denominated in **Gwei**, which represents one-billionth of an ETH. Exorbitant gas fees have led to users seeking alternative methods of capacity and cost reduction.

HIGH DEMAND LEADS TO GAS PRICE VOLATILITY

Source: Etherscan.io as of March 1st, 2022



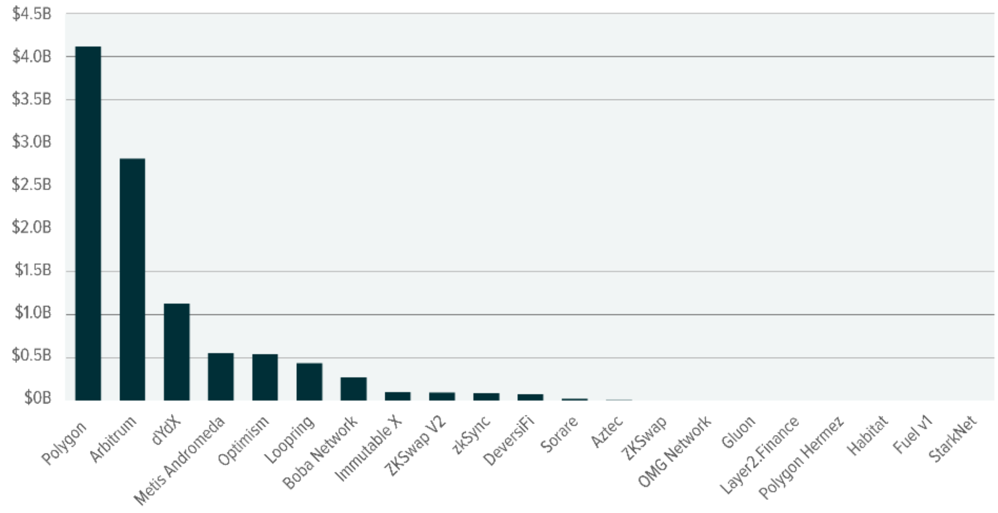
EIP-1559 offers a better pricing structure with more gas price predictability, but it does not guarantee that gas prices decrease. Currently, the solutions used to scale Ethereum cost-effectively include on-chain scaling and off-chain scaling. On-chain scaling involves finding methods that improve cost and throughput on the Ethereum base layer. For example, as part of the Ethereum Consensus Layer rollout, the Ethereum network plans to introduce shard chains. Shard chains refer to the process of splitting a database into multiple sections horizontally to reduce network congestion and increase the number of transactions per second. A shift to Proof-of-Stake is a prerequisite for sharding. In a Proof-of-Work system, sharding would dilute the security properties and allow malicious miners to corrupt individual shards more easily.

Off-chain scaling aims to build alternative scaling protocols on top of Ethereum, which is referred to as Layer 1 (L1). Solutions implemented outside of Ethereum are referred to as Layer 2 (L2). Layer 2s ultimately derive security from the **mainnet,** the primary Ethereum network. These applications generally process individual transactions in a separate state, and they communicate with the Ethereum mainnet for settlement in various ways, depending on the type of solution.

L2 solutions are increasingly popular because they can help process small transactions faster and cheaper while using the Ethereum mainnet for security and transparency. Polygon, which helps developers build scalable DApps with minimal transaction fees, is one of the predominant L2 solutions. Competing smart contract platforms like Solana have had success trading a degree of decentralization for enhanced transaction throughput, however, L2 solutions offer an inexpensive way to transact while remaining in the Ethereum ecosystem. L2s have a sizable amount of total value locked (TVL) or the overall value of crypto assets in their platforms.

THE LAYER 2 SOLUTION ECOSYSTEM HOLDS $10 BILLION IN TOTAL VALUE LOCKED

Source: DeFillama.com & L2beat.com as of March 1st, 2022



ETH's Value: It Fosters a Growth-Oriented Economy for the Network

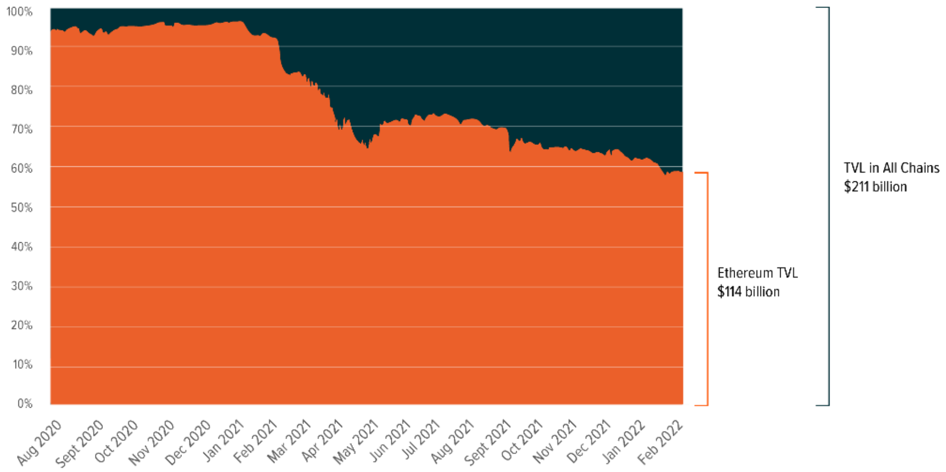
Acting as the settlement currency, ETH derives its value from the demand of the Ethereum network. ETH is commonly used to:

- Pay for transaction or gas fees.
- Interact with DeFi DApps.
- Pay for the deployment of smart contracts into the blockchain.
- Primary unit of account in NFT marketplaces and trading.

With about $114 billion, Ethereum leads the crypto landscape in total value locked within DApps.[5] In DeFi, total value locked is an important metric because it provides insight into the monetary value deposited in the applications and serves as a reliable gauge of sentiment and growth. Locking assets within protocols indicate growth, utility, and user conviction in the ecosystem. Additionally, roughly 9.7 million ETH, the equivalent of about $28 billion, is locked under the Proof-of-Stake validator contract to secure the network in its future state: further reducing the amount of ETH in circulation.[6]

ETHEREUM LEADS THE RACE WITHIN THE $211 BILLION TOTAL VALUE LOCKED IN DEFI

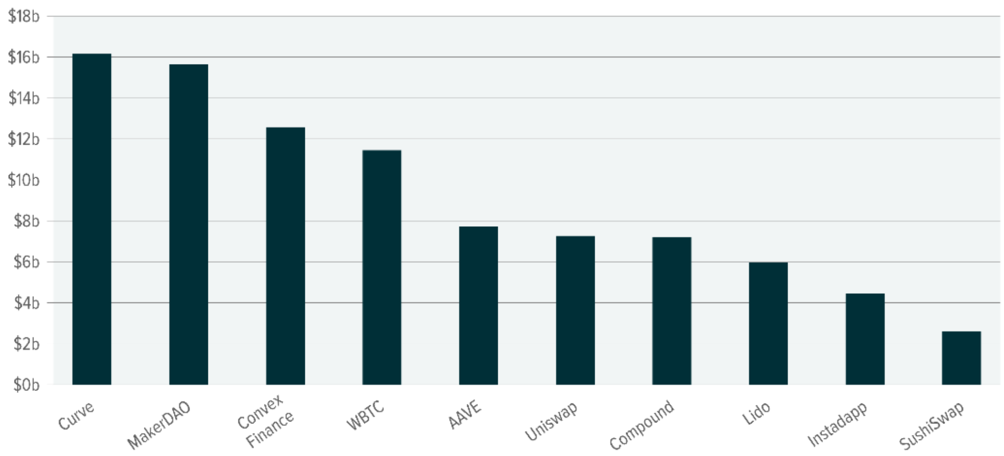
Source: Defillama.com as of March 1st, 2022



What is great about Ethereum is that the Total Value Locked is distributed among many DeFi DApps.

LET'S BREAKDOWN THE TOP 10 CONTRIBUTORS TO ETHEREUM'S $114 BILLION TOTAL VALUE LOCKED IN SMART CONTRACT DAPPS

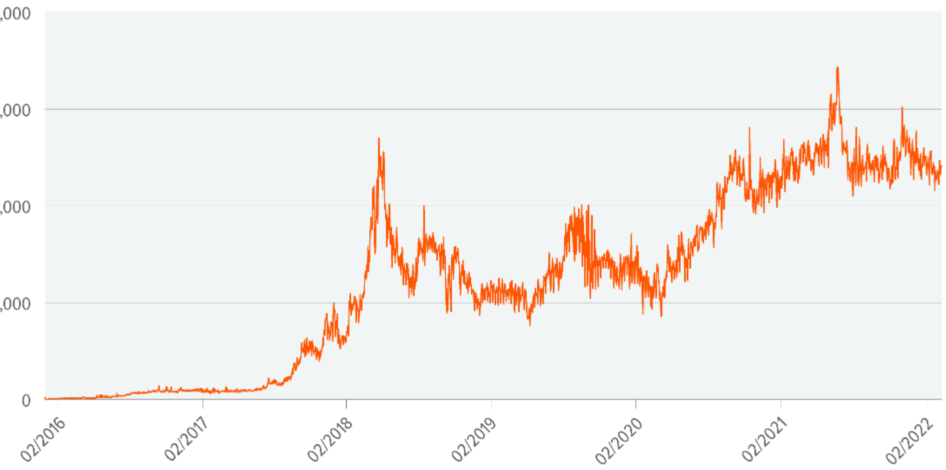
Data Source: Defillama.com as of March 1st, 2022



Additionally, on-chain metrics such as the number of wallets and the number of daily transactions have increased over time, signaling demand for the Ethereum ecosystem. The number of transactions directly correlates with the transaction fees paid.

TOTAL ETHEREUM TRANSACTIONS PER DAY

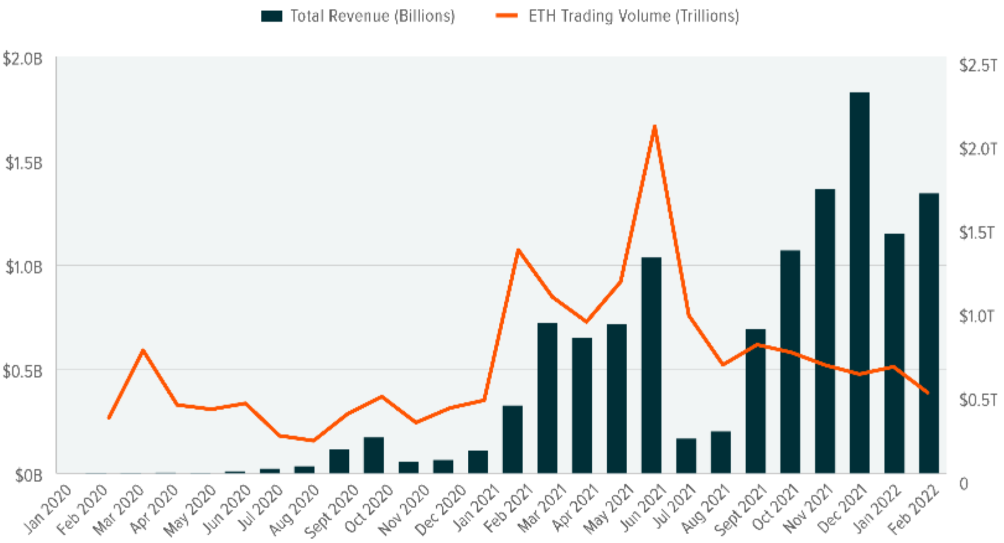
Source: Etherscan.io as of March 1st, 2022



In 2021, Ethereum generated $9.9 billion in revenue via user transaction fees paid and ETH transaction volume totaled $11.5 trillion.[7]

TRANSACTION REVENUE CONTINUES TO GROW ON AN ANNUALIZED BASIS

Data Source: Tokenterminal.com as of March 1st, 2022



Theoretically, ETH's supply is unlimited because there is no limit on coins that can enter circulation in the form of block rewards. EIP-1559 altered ETH's monetary policy because it allows for a variable block reward issuance ratio. A variable ratio is possible because of the effect transaction volume has on the amount of ETH removed from circulation.

With the burning mechanism, the variable issuance rate can decline as network demand increases, and it can cause the token's float to decrease as transaction demand continues to rise.

The impact of the burning mechanism on gas fees and annual issuance adds to the scarcity of in-demand ETH.

Currently, Ethereum's annual network issuance is approximately 4.5%, with 2 ETH per block awarded.[8] Over time, the block reward curve can continue to decrease in the transition to an improved and more scalable version of Ethereum.

Why Ethereum now: A Smart Contract Blockchain with Mechanisms to Create Value and Scalability

To understand Ethereum's growing appeal and value is to recognize what Buterin articulated in his whitepaper: the potential to expand the blockchain's decentralized properties programmatically. For investors interested in exposure to Ethereum, the first successful application of a programmable blockchain, we expect that:

- The value locked within its ecosystem, the utility and interoperability of tokens and smart contracts, and the growing transaction count and its effect on burning ETH can continue to drive value.
- Upgrades such as the transition to Proof-of-Stake and on-chain and off-chain scaling advancements, including the Ethereum Consensus Layer rollout and improvement in Layer 2 applications, give Ethereum scalability. These upgrades will also attract more developers to this growing ecosystem due to its network effect, further increasing demand for ETH's utility.

Ethereum's adaptive features also position it well to play a central role in disruptive movements like the evolution of the internet to Web 3.0, which at its core is a user-owned blockchain ecosystem. Considering developments like these and the demand that they could create for ETH, we view this digital asset and the blockchain network that it fuels as having meaningful growth potential.

Footnotes:

1. CoinMarketCap. (2022, March 1). *Historical snapshot – 01 March 2022.*
2. Watch the Burn. (2022, March 1). *Blocks.*
3. Ultrasound.money. (2022, March 1). *Ultra sound awakening: Track ETH become ultra sound.*
4. Uniswap. (2022, March 1.) *Ethereum: Overview.*
5. DeFi Llama. (2022, March 1). *DeFi TVL rankings: Ethereum.*
6. Etherscan. (2022, March 1). *Contract: 0x00000000219ab540356cBB839Cbe05303d7705Fa.*
7. Token Terminal. (2022, March 1). *Projects: Ethereum.*
8. EthHub. (n.d.) *Ethereum basics: Monetary policy.*
9. Hotchkiss, G. I. (2019, December 19). The 1.x files: The state of stateless Ethereum. *Ethereum Foundation Blog.*
10. Agarwal, A., Smith, C., Wackerow, P., Samani, Q., Joshua, Leung, N. H., Singh, H., & Richard, S. (2022, February 4). Miner extractable value (MEV). Ethereum.

Glossary

Terms are listed in the order in which they appear.

Bitcoin: A digital bearer asset that exists entirely as a ledger balance on the Bitcoin blockchain. It is the native cryptocurrency of the Bitcoin network.

Blockchain: A peer-to-peer shared and continually reconciled distributed ledger that facilitates the recording of transactions and tracking of assets without the need for a trusted intermediary.

Turing complete programming language: Programing language that can perform any computational operation.

Smart contracts: Programmatically executed contracts based on code.

Decentralized Applications (DApps): Decentralized applications built on top of smart contracts that are backed by blockchain technology.

Decentralized financial service applications (DeFi): DApps offering financial instruments without the need for intermediaries. DeFi DApps are powered by smart contracts. DeFi allows users to participate in money market activities such as lending and borrowing via decentralized avenues.

Non-fungible tokens (NFTs): Non-interchangeable and uniquely identifiable assets.

Decentralized autonomous organizations (DAOs): Decentralized organizations whose rules and authority live within a smart contract.

Transactions: A signed data package that stores a message to be sent from an externally owned account. Transactions represent cryptographically signed instructions. A transaction can be viewed as transferring available digital assets to another address, and publishing or executing a smart contract.

States: Describes the current status of all accounts and balances, as well as the data of all smart contracts.

Blocks: Data structures within the Ethereum network containing transaction details. Every new block created contains a reference to its parent, or previous, block.

Ethereum Virtual Machine (EVM): The underlying platform used by developers to create DApps and host accounts and smart contracts. The EVM stores the network's data and keeps the state of the network up to date.

Digital signature: Mathematically derived from a private key and a transaction's hash. A digital signature proves ownership of a private key and the associated public key without having to reveal the private key.

Public-key cryptography: Also known as asymmetric cryptography, it utilizes two distinct but mathematically connected keys, one for encryption and one for decryption where the public key is used to receive ETH, and the private key is used to sign transactions to spend ETH.

Nodes: The distributed network of computers running the Ethereum network software to verify transactions and messages before they enter the blockchain. There are different types of nodes.

Ethereum client: The application needed to run a full node. Nodes essentially run client software, which is available on multiple open-source coding languages. The purpose of the client is to act as the software that verifies transactions against the network's standards.

Gas fee: Transactions in the Ethereum Network come at a cost. Gas fees represent the amount of Ether paid to validate, include, and secure transactions in the blockchain. Gas fees are denominated in Gwei, and the required gas needed to process a transaction is generally based on network demand.

Mining nodes: A special subset of nodes that aggregate transactions together into the blocks that are recorded onto the blockchain for settlement. Mining nodes compete to be the first to solve a challenging mathematical puzzle based on a cryptographic hash function. Miners dedicate large amounts of computational resources to brute-force calculate the result of different inputs through a cryptographic hash function as quickly as possible.

Cryptographic hash function: A one-way function that can be used to map data of an arbitrary length to a deterministic fixed-length result. Cryptographic hash functions include these key properties: 1) They are repeatable; for any input, the resulting output (hash) is always the same. 2) They are one-way functions where it is impossible to derive an input from a given output. 3) The optically random nature of the function makes it impossible to tailor an output by making small adjustments to an input. The mining process relies on computing the result of a cryptographic hash function repeatedly as fast as possible to achieve a certain output. These functions are also used to derive an address from a public key.

Hash: The output of a cryptographic hash function.

Candidate block: A block of pending transactions that a miner is attempting to add to the blockchain by finding a valid Proof-of-Work. After a Proof-of-Work is found, a candidate block becomes a valid block and is added to the chain. Miners typically form candidate blocks by selecting the transactions in the memory pool with the highest transaction fees.

Proof-of-Work: The solution to the challenging mathematical puzzle based on a cryptographic hash function that miners compete to solve. Due to the properties of cryptographic hash functions, the Proof-of-Work is incredibly difficult to find, but any node can trivially verify that the miner expended the computational resources to find this solution. The Proof-of-Work helps resolve disagreements when two blocks are mined simultaneously, and it protects the network by making historical blocks prohibitively expensive to manipulate.

Block time: The time it takes to mine a new block.

Block size: The capacity of data per block.

Block reward: A special transaction that allows the miner to send themself a fixed amount of newly created ETH as a financial incentive for solving the block.

Front running: Detecting profitable arbitrage opportunities within the mempool. The idea is to identify these opportunities and submit transactions with a higher gas limit in order to benefit from the arbitrary opportunity, thus front running the original transaction.

Miner or maximal extractable value (MEV): Refers to the maximum value that can be extracted from block production in excess of the standard block reward and gas fees by including, excluding, and changing the order of transactions in a block.[10]

On-chain: Refers to transactions that occur on the actual blockchain.

Ethereum Improvement Proposals (EIPs): Describes the current standards for the Ethereum network and all updates agreed on. Network builders can propose new ideas and changes to the existing network.

Confirmations: The number of blocks added to the blockchain after a particular transaction was included in a block. The first confirmation is when a transaction is included in a block. Additional confirmation is added every time a new valid block is mined onto the chain.

Forked chain: A blockchain that diverges from a single chain into two different chains. These chains share the same history but reach a point where their newer blocks cease to be the same. Temporary forks occur when two miners mine a block simultaneously but the protocol rules result in this converging back on a single main chain.

Main chain: The blockchain that took the most cumulative work to mine based on the difficulty of the underlying blocks. Typically, the main chain has the most blocks.

ERC-20: An EVM token standard based on smart contracts. ERC-20 tokens provide a common set of rules in order to incentivize composability among tokens.

Stablecoins: Cryptocurrency tokens designed to be pegged to the US Dollar on a 1:1 ratio and meant to stabilize the market by adding liquidity and trading avenues.

Composability: The ability to operate and interact with other like-kind assets.

ERC-721: An EVM token standard based on smart contracts. The key difference between ERC-20s and ERC-721s is the ability to program a non-fungible token and the rules behind it.

Proof-of-Stake: A consensus mechanism where validators must “stake” their assets to confirm and record transactions.

Validators: Network participants who validate and confirm transactions in a Proof-of-stake consensus mechanism.

Slashing: Validator penalties under a Proof-of-Work consensus mechanism where the entire or a portion of the staked assets are seized.

Proposers: Validators that are algorithmically chosen to propose a new block.

Attestors: Validators that are not chosen to propose a block must attest to a chosen validator’s block proposal and confirm the information is as per the standards.

Gwei: Giga-wei or Gwei is often used to describe gas costs on the Ethereum network and represents one-billionth of an Ether.

Mainnet: Term used to describe the main blockchain.