Ethereum (ETH)

INTO THE ETHER

JANUARY 2020

+ An asset primer tackling the fundamentals of the ethereum network
+ A discussion of key-trends and challenges in ethereum
+ An overview of ethereum 2.0 and future scaling solutions

Over the last few years, numerous cryptocurrency projects have come to market, many relying on the ethereum protocol for computational properties and transfer settlement. In this note, we provide an in-depth overview of the ethereum network that launched in 2015 and discuss the core characteristics that set it apart. Ethereum was developed as a decentralized computing platform that allows users to enforce agreements and run applications without a centralized party through autonomous agents known as 'smart contracts.' Smart contracts run on a computational set of instructions and are expected to change the way individuals, businesses, and societies transact through programmable monetary transfers over decentralized applications. That said, as network user transaction count grows and usability improves, ethereum - like other crypto networks - will continue grappling with scalability concerns. Longer-term, the success of ethereum rests on the success of executing against new scalability initiatives, described as "ethereum 2.0."

This report breaks down the discussion of the ethereum network into six parts: Origins, The Protocol, Key Events, Scalability, Adoption, and Conclusion. We'll begin with a background on the launch of ethereum, break down key aspects of the protocol, and delve into the defining moments of the network's history. We'll then take a look at scalability and review developments that address current limitations, and wrap up with a discussion of adoption. Our aim is to provide a holistic overview of the ethereum network and contextualize its place in the broader cryptocurrency space.

PRICE	MARKET CAP
$172	$19B
TX/DAY	TOTAL ETH SUPPLY
526K	109M

BACKGROUND DATA

Creator: Vitalik Buterin
Launch: July 2015
Consensus algorithm: PoW

SOCIAL DATA

Github contributors: 445
Github commits (1Y): 811
Reddit subscribers: 450k
Daily tweets: 3.9k

BLOCKCHAIN DATA

Market dominance: 7.5%
Hashrate: 162TH/s
Unique addresses: 86M
Daily total nodes: 8,005

1Y PRICE CHART

Data as of 28 Jan 2020
Source: etherscan, bitinfocharts, github, reddit

Table of Contents

I. Origins

The concept of digital money existed long before the advent of bitcoin, tracing its roots as far back as the early-1980s with David Chaum's paper "Numbers Can Be a Better Form of Cash than Paper."[1] Chaum first proposed the idea of an electronic cryptocurrency, 'ecash,' which ignited the Cypherpunk movement of the 1990s, almost a decade later. Many of these cypherpunks shared an ideological opposition to centralized control and censorship, which led to endeavors focused on a censorship-resistant monetary system leveraging cryptography. An early member of the cypherpunk movement, Nick Szabo, introduced the concept of digitally-enforced, trustless transactions with "smart contracts." Nearly 20 years later, the introduction of bitcoin inspired the launch of a new platform that would focus on smart contracts: the ethereum network. Envisioned by several crypto enthusiasts, listed in figure 1 below, Vitalik Buterin released the ethereum white paper in 2013, concluding that the design of bitcoin was functionally limited by its specific operation as a peer-to-peer currency.

Figure 1: Co-founders of ethereum

Member	Role
Vitalik Buterin	- co-founder and writer of the Bitcoin Magazine (2012) - authored and published the ethereum white paper (2013) - co-founder of ethereum (2014)
Mihai Alisie	- co-founder and editor-in-chief of the Bitcoin Magazine (2012) - co-founder, chief innovation officer, and VP of ethereum (2014) - founder of the AKASHA Project (2015)
Anthony Di Iorio	- co-founder of ethereum (2014) - founder and CEO of Decentral Inc.(2014) and Jaxx (2018) - chief digital officer of the Toronto Stock Exchange (2016)
Charles Hoskinson	- co-founder, CEO of ethereum (2014) - co-founder of IOHK (2015)
Amir Chetrit	- co-founder of Bitcoin Magazine (2012) - co-founder of ethereum (2014)
Joseph Lubin	- co-founder of ethereum (2014) - founder of ConsenSys (2015)
Gavin Wood	- co-founder and CTO of ethereum (2014) - authored the ethereum yellow paper and designed the Solidity smart contract programming language (2014) - founder of Parity Technologies (2015)
Jeffrey Wilcke	- co-founder of ethereum (2014) - co-founder of Grid Games (2018)

Source: Kraken Intelligence

Anticipating a world with broader application of blockchain technology, Vitalik Buterin created ethereum to be a decentralized application[2] platform where one base protocol could seamlessly enable thousands of individual applications. Pursuing the vision of a "world computer," the ethereum team modified the original bitcoin protocol and blockchain design to support smart contracts such as a Turing-complete[3] programming language acting as a generalized, transaction-based state machine.[4]

1 "Numbers Can Be a Better Form of Cash than Paper" (https://link.springer.com/chapter/10.1007/3-540-57341-0_61)

2 *Decentralized applications (dapps) are applications designed to run on peer-to-peer networks rather than on a centralized server.*

3 *A computer programming language that can perform any computational problem, by recognizing an input to yield an output.* (https://www.computerhope.com/jargon/t/turing-completeness.htm)

4 *A state machine is a device capable of reading an input and producing a new state, or output, based on the implemented changes dictated in the input. (https://cointelegraph.com/ethereum-for-beginners/what-is-ethereum#is-ethereum-like-bitcoin)*

II. The Protocol

Ethereum utilizes the concept of 'accounts' and 'state' in place of bitcoin's unspent transaction output (UTXO) model. Under the UTXO model, a balance can be transacted, split, or combined, and are associated with a wallet holder's "balance" simply through their ability to sign a transaction that spends the UTXO. Under ethereum's state model, every account retains a balance state, and each transaction results in a single output for transfers or expenditures. The UTXO model is akin to that of a cash transaction where a serial numbered bill must be transferred from one individual to another, for the receiver to have the right to spend the money. However, ethereum's state model is similar to that of a bank transaction where a bank account will recognize the 'credits' under an individual's name and when transfered, the recipient has the right to use the credits. Ethereum's account-based model recognizes two types of accounts:

1. externally-controlled accounts; and
2. contract-controlled accounts.

Tracking the balance of an account is intuitive, as the network verifies the state of an account before approving any transactions, much like debit cards or ATM machines that check the total balance of a user's account before approving an expenditure. Now that we understand the state model, let's delve deeper into the protocol infrastructure, which can be broken down into several core features: smart contracts, Solidity, Ethereum Virtual Machine (EVM), gas, miners, nodes, and proof-of-work consensus (PoW).

- **Smart contracts** are programmable contracts that allow the trustless execution of codified terms without the need for a third party. They are seen as autonomous agents that manage the exchange of value in the ethereum network by self-executing when specified conditions are met, similar to the concept of an escrow account. Although the bitcoin protocol also provides for the creation of smart contracts, some argue it lacks flexibility relative to ethereum as it is limited to the transfer of currency and was not intended as a platform for smart-contracts. Smart contracts are entirely dependent on previous events and states, in order for the network of nodes to validate and maintain consensus on the newly mined blocks. Smart contracts have their own address in order to receive and send ether, and may employ oracles, or intermediaries that feed external information to the smart contracts. Because smart contracts can only access information broadcast on the blockchain, oracles are necessary to leverage data from the outside world for smart contracts that require such data. In these oracle-dependent smart contracts, certain external data providers are explicitly defined to maintain the consistency and authenticity of the data source. Some consider oracles a primary fault-point for the ethereum network, but efforts are underway to improve the integrity of this weakness in smart contract execution.[5]

- **Solidity** is a programming language native to ethereum, used in the implementation of smart contracts which executes the EVM. It has similarities to Javascript, C++, and Python, making it widely accessible for programmers.[6]

- **The Ethereum Virtual Machine (EVM)** is a Turing-complete virtual machine, which performs computations of arbitrary complexity.[7] The EVM's design is the foundation for ethereum as a programmable application platform. The EVM operates inside of every ethereum client and is used by nodes and miners to validate transactions and to store, process, and reconcile state in exchange for ether as **gas**.

5 "What are Oracles? Smart Contracts, Chainlink & "The Oracle Problem"" (https://blockonomi.com/oracles-guide/)
6 "From Javascript to Solidity" (https://medium.com/coinmonks/from-javascript-to-solidity-12317e8965de)
7 "Surprisingly Turing-Complete" (https://www.gwern.net/Turing-complete)

- **Gas** represents the number of computational steps involved in executing a smart contract. Payable in ether, the gas price is the amount of ether paid by the sender on every unit of gas, usually measured in gwei, with 1 ether being the equivalent of 1,000,000,000 gwei.[8] Ether acts as both the fuel that pays for the execution of decentralized applications and as a transactable currency. The use of gas encourages miners to process smart contracts and simultaneously discourages developers from executing inefficient and clunky programs. Ether is currently mined using proof-of-work at a constant rate of 2 ETH per block [9] and the total supply of ether remains unconstrained with over 109M ether in circulation.[10] Ethereum employs a **gas limit** in place of a fixed block size, effectively capping the volume of transactions and smart contract execution capacity.

- **Nodes** (computers) store replica copies of the blockchain and broadcast new transactions over a network of peer nodes. When someone executes a valid transaction, a node propagates the transaction information to other network nodes, which collect these transactions in the memory pool (mempool), a queue of unconfirmed transactions.

- **Miners** are nodes that compete to introduce new blocks onto the blockchain by confirming and packaging transactions from the mempool.[11] Miners are rewarded with newly minted ether and transaction fees for each block they successfully mine. The process of mining involves an expenditure of computing power to create a valid proof-of-work.

- **Proof-of-Work (PoW) consensus** is the set of network rules that determines whether blocks and transactions are considered valid. This process is carried out by **nodes** and **miners**, the former being responsible for propagating and storing of the blocks in the blockchain and the latter for introducing new blocks by confirming transactions from the mempool.[12] Miners receive block rewards, or newly minted ether along with transaction fees, with each new block successfully mined. The ethereum network was designed with a PoW algorithm known as Ethash to make mining fairer by skewing towards GPU hardware. However, due to the computational effort expended with PoW and for greater scalability, the ethereum network will migrate to a Proof-of-Stake (PoS) mechanism. The gradual transition to PoS has been scheduled since 2018, but has seen multiple delays.

For a closer look at the mining process and proof-of-work consensus, we recommend our Cryptocurrency Mining Primer.

8 Definition of Gwei (https://gwei.io/)
9 *As outlined in the Constantinople upgrade.*
10 Total Ether Supply (https://etherscan.io/stat/supply)
11 *A pool of unconfirmed transactions.*
12 Kraken Intelligence Cryptocurrency Mining Primer (https://blog.kraken.com/wp-content/uploads/2019/04/Cryptocurrency-Mining-A-Primer-April-2019.pdf)

III. Key Events

2013

ethereum white paper published: the development of the ethereum network was split into four distinct phases. Frontier was the first official phase that launched the network. The second phase, Homestead, was the first major upgrade to the network and during this phase the network experienced three hard forks - the DAO fork, Tangerine Whistle, and Spurious Dragon. All three forks were in response to major attacks on the network. The third phase was named Metropolis, during which two main upgrades were made to the network, known as Byzantium and Constantinople. The last known planned phase is Serenity, or ethereum 2.0, which introduces important technological upgrades such as the Beacon Chain, sharding, plasma, and Casper. Each stage implemented major updates designed to optimize the system and efficiently address issues that arose. Details of each stage are outlined in figure 2 below.

Figure 2: Ethereum roadmap

Stage	Name	Block	Date	Main updates
1.	**Frontier**	0	30-Jul-15	First phase: pre-sale of ethereum
2.	**Homestead**	1,150,000	14-Mar-16	Second phase: experienced The DAO attack and led to hard-fork of the network
	DAO	1,920,000	20-Jul-16	Hard fork into two chains following The DAO attack: ethereum and ethereum classic
	Tangerine Whistle	2,463,000	18-Oct-16	The first hard fork in the two-round hard fork response to DoS attacks on the network in Sept-Oct 2016. Addressed immediate network health issues resulting from attacks through gas cost changes (EIP 150) and state clearing (EIP 158)
	Spurious Dragon	2,675,000	22-Nov-16	The second hard fork in the two-round hard fork response to DoS attacks on the network in Sept-Oct 2016. Addressed less immediate issues such as replay attack protection (EIP 155), EXP cost increase (EIP 160), state trie clearing (EIP 161), and contract code size limit (EIP 170)
3.	**Metropolis**			Third phase divided into two stages: Byzantium and Constantinople
	Byzantium	4,370,000	16-Oct-17	Introduction of ZK-Snarks, delay of difficulty bomb by 1 year, reduction of block reward from 5 ETH to 3 ETH
	Constantinople/ St.Petersburg	7,280,000	28-Feb-19	Delay of difficulty bomb by 1 year and reduction of mining reward from 3ETH to 2 ETH
4.	**Serenity**	-	-	Last known planned phase of ethereum 2.0: introduction to the Beacon Chain, sharding, plasma, and Casper

Source: Ethereum Foundation, blockexplorer.com

2014

ether pre-sale: the pre-sale for the ether token was released to the public, utilizing the bitcoin blockchain as a purchase database, with bitcoin accepted in exchange for ether tokens.[13,14] At a token price of 2,000 ether per bitcoin, or $0.31 per ether, the pre-sale raised more than $18M, with over $2.3M raised within the first 12 hours of the sale.[15,16] On September 2nd, pre-sale investors received a total of 60M ether, and an additional 12M was allocated to the developers of the network and the Ethereum Foundation.[17]

2015

launch of Frontier: ethereum launched its initial version of the protocol, Frontier. During this year, ethereum saw tremendous growth in demand as the protocol underwent constant improvement, attracting developers to its accessible platform.

2016

the DAO attack and Ethereum Fork: the first network attack on ethereum with The DAO hack in June. The DAO was the name of a particular Decentralized Autonomous Organization,[18] and experienced an attack through a recursive bug identified in the smart contract of The DAO.[19] The Ethereum Foundation and network users decided to find a solution to nullify the stolen ether, and Vitalik Buterin proposed a soft-fork to make any stolen ether transactions invalid. However, network consensus was to push forward with a more aggressive hard-fork of the ethereum network, effectively reversing all transactions related to The DAO and rewriting history to return all funds back to the respective owners. This was a controversial decision perceived by some as a bail-out by a central party, and created an ideological rift in the network. A group of people who believed it ruined the integrity of ethereum and the tenets of cryptocurrency remained on the original chain, now known as ethereum classic. However, around 90% of the network hashpower moved on with the hard-fork, supporting the ethereum network of today.[20] This attack raised concerns about the stability and long-term outlook of the network as an autonomous, truly decentralized application platform.

13 "Background on the Mechanics of the Ether Pre-sale" (https://blog.ethereum.org/2014/07/09/how-to-make-a-purchase-in-the-ether-presale/)

14 "Ether Sale: A Statistical Overview" (https://blog.ethereum.org/2014/08/08/ether-sale-a-statistical-overview/)

15 "Ethereum Raises 3,700 BTC in First 12 Hours of Ether Presale" (https://cointelegraph.com/news/ethereum-raises-3700-btc-in-first-12-hours-of-ether-presale)

16 Ethereum ICO Stats (https://icodrops.com/ethereum/)

17 Ethereum total supply and market capitalization (https://etherscan.io/stat/supply)

18 *A Decentralized Autonomous Organization (DAO) is an organization that seeks to eliminate hierarchical management in institutions by replacing the operational middlemen with a DAO on the ethereum platform.*

19 "Understanding The DAO Attack" (https://www.coindesk.com/understanding-dao-hack-journalists)

20 "From Crowdfunded Blockchain to ICO Machine: An Ethereum Price History" (https://blog.sfox.com/from-crowdfunded-blockchain-to-ico-machine-an-ethereum-price-history-ddb31c3134c4)

2017

the rise of ICOs: the popularization of ICOs enabled developers around the world to raise capital for project developments by creating and issuing their own tokens on the ethereum blockchain. Investors would send either fiat or cryptocurrencies to developers in exchange for newly minted tokens. The ease of creating and deploying applications for ICOs on the platform ultimately led to an explosion of ICOs flooding the market and was a primary driver of the bull run of 2017. Consequently, high profile ICOs began to take place as the market gained traction in the latter half of the year, raising over $6.4B in funding in 2017, $1.7B of which was raised in December alone. Some of the largest ICOs to date are listed in figure 3. [21,22,23] A majority of these projects successfully raised millions in capital, creating a flurry of demand for ether, resulting in a gain of over 9,000% in 2017 for ether holders.

ERC-20 token standard formalized: Ethereum Request for Comment (ERC)-20 is the technical standard used for smart contracts in creating fungible utility tokens on the ethereum network. It's a common set of rules implemented to program tokens to function, improving interoperability between different projects on the network. Most tokens issued during the ICO boom were created as an ERC-20 token.

launch of CryptoKitties: a notable event that contributed to the congestion of network activity was the creation of CryptoKitties, one of the earliest viral dapps on the ethereum network. CryptoKitties is a game implementing non-fungible (ERC-721) tokens represented in the form of virtual kittens, or 'CryptoKitties.' The game leverages smart contracts to breed and sell CryptoKitties on the blockchain and is one of the most well-known implementations of a non-fungible token/digital asset[24] used in the form of a game.

Figure 3: Major ICOs to date

Project	Size
EOS	$4.2B
Telegram	$1.7B
Petro	$735M
TaTaTu	$575M
Dragon	$320M
Hdac	$258M
Filecoin	$257M
Tezos	$232M
Sirin Labs	$158M
Bancor	$153M
The DAO	$152M
Polkadot	$140M
Status	$108M
BAT	$35M

Source: project websites, thecoinoffering

2018

Scalability Research and Development Subsidy Programs announced: the Ethereum Foundation announces grants for the development of layer-2 scaling strategies on ETH2.0.[25]

partial proof-of-concept released for sharding: Vitalik Buterin releases the 'fork choice rule,' a code repository that dictates the interaction of shards with the main chain and enabling efficient scaling.[26]

Casper FFG code released on Github: ethereum's PoS implementation, Casper the Friendly Finality Gadget, code for v1 of ETH2.0 is released on Github.

2019

launch of Raiden Network on mainnet: Raiden Red Eyes, an off-chain payment channel network, goes live on ethereum mainnet. The Raiden Network enables fast, scalable, and cheap decentralized payments.[27,28]

Constantinople/St. Petersburg upgrade: the ethereum network underwent its scheduled Constantinople/St. Petersburg update at block 7,280,000 which reduced the block reward by 33% and paved the way for ethereum 2.0.[29]

Istanbul hard fork: the ethereum network went through its scheduled mainnet upgrade at block 9,069,000.[30] This upgrade implemented 6 backward-compatible changes which set the groundwork for ethereum 2.0. Main changes include distributed denial-of-service (DDoS) resilience, interoperability with other equihash PoW tokens, and adjustment of gas costs for greater network bandwidth.[31]

21 "ICO Scams – Fake Initial Coin Offering Tokens List" (https://bitcoinexchangeguide.com/top-6-ico-fundraisers-eos-telegram-dragon-huobi-hdac-and-filecoin/)
22 "Top 10 Biggest ICOs" (https://www.bitcoinmarketjournal.com/biggest-icos/)
23 Basic Attention Token ICO (https://cryptoslate.com/coins/basic-attention-token/)
24 *Individually unique tokens that are not interchangeable; contrary to cryptocurrencies like bitcoin that are mutually interchangeable.*
25 "Ethereum Scalability Research and Development Subsidy Programs" (https://blog.ethereum.org/2018/01/02/ethereum-scalability-research-development-subsidy-programs/)
26 "Vitalik Releases Partial Proof-of-Concept for Ethereum 'Sharding' Tech" (https://www.coindesk.com/vitalik-releases-partial-proof-concept-ethereum-sharding-tech/)
27 "Red Eyes Mainnet Release Announcement" (https://medium.com/raiden-network/red-eyes-mainnet-release-announcement-d48235bbef3c)
28 "Raiden Network: Vision, Challenges and Roadmap" (https://medium.com/raiden-network/raiden-network-vision-challenges-and-roadmap-593dfa34b868)
29 "Ethereum Constantinople/St. Petersburg Upgrade Announcement" (https://blog.ethereum.org/2019/02/22/ethereum-constantinople-st-petersburg-upgrade-announcement/)
30 "Road to Istanbul: ETH Hard Fork Explained" (https://medium.com/superorder/road-to-istanbul-eth-hard-fork-explained-d0101377dcc7)
31 "Ethereum's Istanbul Hard Fork Is Now Live" (https://www.coindesk.com/ethereums-istanbul-hard-fork-is-now-live)

IV. Scalability

Scaling has been, and remains, one of ethereum's greatest challenges. During booming market conditions and the ramp-up in the creation of dapps and ICOs in late-2017, the network began experiencing scaling difficulties. One notable example that laid bare the network's failure to scale was the launch of CryptoKitties on November 28, 2017. CryptoKitties was the first decentralized application (dapp) to go viral such that amateur crypto users could interact with the platform. As the popularity of CryptoKitties congested the ethereum network with an extremely rapid increase in transactions, unprocessed transactions grew sixfold and total activity on the dapp accounted for nearly 12% of all transactions on the ethereum network in the first week of December 2017.[32,33]

To meet the demands of the real-world while preserving decentralization, Vitalik Buterin announced his vision for ethereum 2.0, which outlined a set of upgrades slated to take place over the coming years with a focus on improving network security, privacy, and scalability.

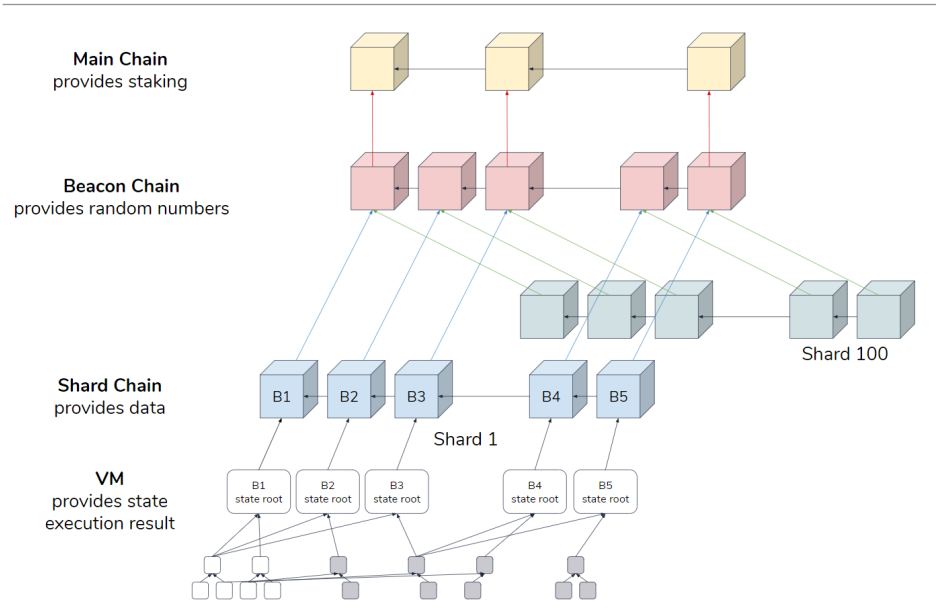
Ethereum 2.0

Ethereum 2.0, also known as Serenity, is a network upgrade that seeks to achieve all three elements of the blockchain trilemma: security, scalability, and decentralization.[34,35] To accomplish this, its main components - the Beacon Chain, Proof-of-Stake (PoS) consensus protocol, sharding, and eWASM - work together to move the majority of computational effort off the main chain.

- **The Beacon Chain** is the core of Ethereum 2.0 and a vital chain running in tandem with other chains, cross-linking the main chain with all shard chains.

- **Proof-of-Stake (PoS) consensus protocol** is an alternative consensus mechanism to the current Proof-of-Work (PoW) mechanism, which assigns the right to create a block through a lottery process rather than through computational expenditure. Consequently, PoS should theoretically encourage decentralization by allowing validators to simply stake their ether balance. The ethereum network plans to gradually transition to a PoS consensus protocol from the current PoW mechanism through the implementation of a hybrid consensus mechanism with **Casper Friendly Finality Gadget** (FFG). Under PoS, misbehaving validators will have their staked coins taken away (slashed) and barred from future staking activities. Though PoS systems are not immune to 51% attacks, compromising the security model relies on a significant acquisition of the circulating currency supply. This exposes the attacker to great economic loss, as attacking the network would likely result in the value of all their staked coins plummeting if users catch on and lose confidence in the protocol itself.[36]

Figure 4: Ethereum 2.0 chain structure



Source: Hsaio-Wei Wang

32 "The Ethereum Network is Getting Jammed Up Because People are Rushing to Buy Cartoon Cats on Its Blockchain" (https://qz.com/1145833/cryptokitties-is-causing-ethereum-network-congestion/)
33 Top 10 ETH Contracts By Transaction Count (https://ethgasstation.info/gasguzzlers.php)
34 "Ethereum Co-Founder Vitalik Buterin Weighs in on Blockchain Improvement & Scaling Issues" (https://cryptovest.com/news/ethereum-co-founder-vitalik-buterin-weighs-in-on-blockchain-improvement--scaling-issues/)
35 Ethereum Github on Serenity (https://github.com/ethereum/wiki/wiki/Sharding-roadmap#strongphase-3strong-light-client-state-protocol)
36 "Responding to 51% attacks in Casper FFG" (https://ethresear.ch/t/responding-to-51-attacks-in-casper-ffg/6363)

- **Sharding** is a method of scaling on-chain transaction throughput by splitting the network's state information into partitions with their own independent state and transaction history, or 'shards.' These shards will make up a chain, with reference points through the Beacon chain, that will act as the layer on which all user transactions take place on the record. This architecture allows the synchronous processing of thousands of sharded transactions, splitting up validation responsibilities across the widespread network of nodes, with no validators required to run the entire network on their server. Each shard will include an **eWASM**-based virtual machine, the equivalent of today's Ethereum Virtual Machine. An eWASM, or Ethereum-flavored WebAssembly, is an engine that executes smart contracts.[37] Currently, there is no developer consensus on the complete replacement of the EVM, but developers plan to allow users to choose between the two, if eWASM is later implemented.[38]

Eight teams are spearheading the development of ethereum 2.0, as shown in figure 5 below.[39]

Figure 5: Developers of ethereum 2.0

Developer	Description	Ethereum 2.0 clients
ChainSafe Systems	Blockchain research & development startup with consulting services	Lodestar
Harmony	Ethereum's original Java client, formerly known as Ether Camp	Harmony
Parity Technologies	Blockchain infrastructure company responsible for the second most popular Ethereum client on the platform 'Parity Ethereum'	Shasper
PegaSys	Blockchain protocol engineering company; Supported by Consensys	Artemis
Prysmatic Labs	Company developing Ethereum's first sharding client	Prysm
Sigma Prime	Information security and blockchain technology consulting company	Lighthouse
Status	Messaging platform and mobile browser for users on the Ethereum network	Nimbus
Ethereum Foundation	Python client for the Ethereum network	Trinity

Source: Coinspeaker.com, coindesk.com, Prysmatic Labs, Trinity Ethereum,

As part of the network transition to ethereum 2.0, a major network upgrade under the name 'Istanbul' went live at block 9,069,000. Though there are more updates to follow, this upgrade rolled out significant improvements that would set the foundation for ethereum 2.0 and the PoS consensus algorithm. Before the launch of the beacon chain, Programmatic Proof-of-Work (ProgPoW) will be introduced as a transitional measure prior to migrating to a PoS system.[40] The current PoW algorithm, Ethash, will be replaced by ProgPoW to close the hardware efficiency gap between ASICs and commodity GPUs. This is intended to resist centralization brought forth by the PoW protocol.[41]

The ethereum 2.0 roadmap is split into three main phases and addresses layer 1 and layer 2 scalability. First, layer 1 (on-chain) improvements are focused on efficiency, throughput, and security. Second, layer 2 (off-chain) improvements focus on scaling the network beyond the limitations of the one base chain. Layer 1 scalability solutions impact the foundational blockchain layer of the protocol while layer 2 solutions operate on top of this foundation.

In order to improve scalability, core developers of ethereum are contributing improvements to both layers 1 and 2 of the network, some of which are outlined in the ethereum 2.0 roadmap. Scaling solutions aim to simplify the mission-critical base layer, while pushing complex functionality further up the stack. In the future, greater weight will be placed on innovation and development in the second layer.

37 "Serenity - The Vision of Ethereum 2.0" (https://etherworld.co/2019/01/04/serenity-the-vision-of-ethereum-2-0/)
38 "Serenity - The Vision of Ethereum 2.0" (https://etherworld.co/2019/01/04/serenity-the-vision-of-ethereum-2-0/)
39 "8 Teams Are Sprinting to Build the Next Generation of Ethereum" (https://www.coindesk.com/next-gen-buidlers-the-8-teams-working-on-ethereum-2-0)
40 "Road to Istanbul: ETH Hard Fork Explained" (https://medium.com/superorder/road-to-istanbul-eth-hard-fork-explained-d0101377dcc7)
41 Kraken Intelligence Cryptocurrency Mining Primer(https://blog.kraken.com/wp-content/uploads/2019/04/Cryptocurrency-Mining-A-Primer-April-2019.pdf)

1. Layer 1 (on-chain) scalability solutions on the ethereum network include the Casper PoS protocol, sharding, and zkSTARKs. Zero Knowledge Scalable Transparent Argument of Knowledge (zkSTARK) is a method of proving the existence of something without exposing the underlying information, through the use of zero-knowledge proofs. An implementation of this technology would create an avenue for privacy and scalability, as it provides fast computations and smaller proofs while protecting sensitive data.[42] The Casper PoS protocol and sharding are part of the ethereum 2.0 roadmap while zkSTARKs is included in future development plans post-ethereum 2.0.[43,44]

2. Layer 2 (off-chain) scalability solutions include sidechains,[45] state and payment channels,[46] and Truebit.[47] Off-chain scalability would move computational effort off the main chain while retaining the decentralized security benefits offered by the main blockchain. Plasma, or sidechains, is one such solution developed by Vitalik Buterin and Joseph Poon. It enables faster transactions and lower transaction fees by the creation of 'child-chains.'[48] Various iterations of Plasma are currently under development.

Another layer 2 solution is **state and payment channels**. A payment channel is the idea behind the Lightning Network of bitcoin, where payment transactions are made off-chain. State channels are similar to payment channels but have the benefit of smart contract operability, by enabling state updates off-chain. Both channels can be included onto the main chain by submitting the final state of transactions and closing the channel.[49] Ethereum's Raiden Network is an example of a state channel, which will likely complement and operate on Plasma sidechains.[50]

The last proposed solution is Truebit. Whereas Plasma and Raiden work to increase total transaction throughput, Truebit addresses computationally complex transactions that would be too expensive to conduct on the main chain. It alleviates the main chain from computational weight by taking it off-chain.[51] The workload of computation verification will be shifted onto a separate network, only utilizing the ethereum blockchain for disagreement settlements, significantly lowering the workload placed on the main chain.[52] Truebit approaches scaling from a different angle and seeks to address transaction complexity rather than transaction count.

3 phases of ethereum 2.0

+ **Phase 0:** The first phase is the launch of the beacon chain. Ethereum 2.0 will implement PoS and sharding on this new beacon chain. As seen in figure 4, this will lead to the creation of three distinct chains - the main chain, the beacon chain, and the shard chain. The beacon chain will run in tandem with other chains, cross-linking the main chain with all sharding chains. Shard chains will act as the layer where user transactions are placed and recorded. The beacon chain will link to shard chains, signaling new blocks that can be added onto the main chain. Network validators will identify and sign shard chain blocks and their crosslink to include on the main chain. A crosslink is a set of signatures attesting to a shard chain block's inclusion into the beacon chain. These three chains, synchronizing and communicating in parallel with one another, will result in speed and scalability as transactions and subsequent operations are moved off the main chain. The main chain will provide staking, the beacon chain will be responsible for blockchain validity, finality, as well as validator registration, and the shard chain will account for all transaction data on the network. The concept of block finality included in the beacon chain is akin to the concept of block confirmations in a PoW network. The deeper the block is embedded into the blockchain, the more finalized it is, making the block more irreversible and resilient against 51% attacks. The beacon chain will use the Casper FFG overlay for finality.[53]

42 "Starkware Industries Presents zk-STARKS for Supercharged Blockchain Scalability, Privacy, &..." (https://hackernoon.com/starkware-industries-presents-zk-starks-for-supercharged-blockchain-scalability-privacy-c42e15a74f98)
43 "Buterin Lays Out Ethereum's Next 3-5 Years, Explains Sharding" (https://www.ethnews.com/buterin-lays-out-ethereums-next-3-5-years-explains-sharding)
44 "The Year in Ethereum" (https://medium.com/@jjmstark/the-year-in-ethereum-87a17d6f82760)
45 "Plasma: Scalable Autonomous Smart Contracts" by Joseph Poon and Vitalik Buterin (http://plasma.io/plasma.pdf)
46 "Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit" (https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4)
47 "Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit" (https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4)
48 "Plasma: Scalable Autonomous Smart Contracts" by Joseph Poon and Vitalik Buterin (http://plasma.io/plasma.pdf)
49 "Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit" (https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4)
50 "Understanding Ethereum Scaling — Categorizing projects by approach adopted" (https://medium.com/matic-network/understanding-ethereum-scaling-categorizing-projects-by-approach-adopted-97c79b25eb55)
51 "Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit" (https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4)
52 "Inside TrueBit: Ethereum's Lesser-Known Scalability Effort" (https://www.coindesk.com/inside-truebit-ethereum-scalability-effort)
53 "Blockchain Finality- Proof of Work and Proof of Stake" (https://medium.com/coinmonks/blockchain-finality-pow-and-pos-35915a37c682)

The Capser FFG protocol is one of the core upgrades to be released in ethereum 2.0. In addition to finality, it will migrate the network to a PoS system. To do this, validators must submit a deposit of 32 ether into a smart contract on the current PoW main chain. This will create a receipt proving validator 'membership' on the beacon chain, enabling validator participation.[54] Unlike the PoW consensus method which requires massive computational power, in PoS, the deposit, or 'stake', determines a node's chance at block validation. Once validators stake their coins, they join a queue and eventually migrate into the pool of active validators.[55] Similar to PoW miners, active validators sign off on blocks and crosslinks, confirming valid transactions. While validators only manage the beacon chain in phase 0, they are expected to also handle shard chains from phase 1 onwards.

Another development in phase 0 is the introduction of Beacon ether (BETH), a new asset for stakers to use on the beacon chain. BETH will be released as the validation reward of the beacon chain, and later for shards, or can be purchased through a deposit of 1 ETH per BETH.[56] As the initial iteration of the beacon chain in this phase will not yet support sharding, smart contracts, and asset transfers, BETH coins cannot be withdrawn until the execution of sharding is implemented in phase 2.[57]

+ **Phase 1:** Once the beacon chain is implemented in phase 0, the development community will shift focus to implementing shard chains. This phase will aim to create consensus on the structure of shard chains, more than the specific execution of the technology. Sharding will break down state information into smaller 'shards' and achieve the network's goal of greater scalability and speed. At this stage, shard chain blocks are expected to be premature in their structure, not yet including concepts like accounts, assets, or smart contracts.[58] These blocks will be mere collections of data, verified by shard validators who will then crosslink the block into the beacon chain. The validity of a crosslink will be proven by validators' consensus. Specifications on phase 1 are still in development, but crosslinking is expected to support cross-shard communication past phase 2.[59]

+ **Phase 2:** In this phase, shard chains will transition into a structured chain state that supports smart contracts and asset transfers. Each shard will have an eWASM-based virtual machine and state rent may also be implemented, which will require developers and users to pay 'rent' for storage on the eWASM-based virtual machine.[60] This is to encourage unloading of unused information from the state to shift the cost burden from full nodes to users over time.[61] Phase 2 is regarded as the final stage of Serenity as it completes the upgrade of the base layer, and this phase is set to take place around 2021.[62]

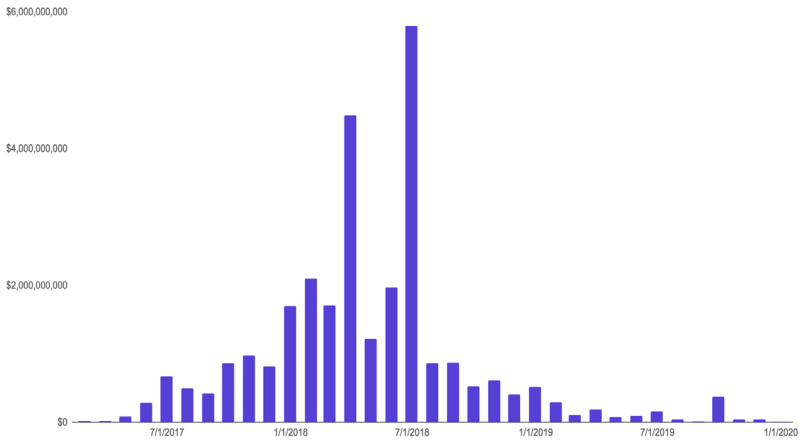
54 "Two Point Oh: Explaining Validators" (https://our.status.im/two-point-oh-explaining-validators/)
55 "The Year in Ethereum" (https://medium.com/@jjmstark/the-year-in-ethereum-87a17d6f8276)
56 "What to Expect When ETH's Expecting" (https://hackernoon.com/what-to-expect-when-eths-expecting-80cb4951afcd0)
57 "What to Expect When ETH's Expecting" (https://hackernoon.com/what-to-expect-when-eths-expecting-80cb4951afcd0)
58 "What to Expect When ETH's Expecting" (https://hackernoon.com/what-to-expect-when-eths-expecting-80cb4951afcd0)
59 "What to Expect When ETH's Expecting" (https://hackernoon.com/what-to-expect-when-eths-expecting-80cb4951afcd0)
60 "What to Expect When ETH's Expecting" (https://hackernoon.com/what-to-expect-when-eths-expecting-80cb4951afcd0)
61 "What to Expect When ETH's Expecting" (https://hackernoon.com/what-to-expect-when-eths-expecting-80cb4951afcd0)
62 "Ethereum 2.0 (Serenity) Kicks Off "Feature Complete" Pre-Release" (https://www.investinblockchain.com/ethereum-serenity-kicks-off-feature-complete-pre-release/)

V. Adoption

In the volatile market of cryptocurrencies, one way to measure the dominance and strength of a network is through the growth of adoption. One way to measure adoption can be improvements on the platform, and we look to ethereum's developer community to see on-going signs of activity. As of early-January 2020, the go-ethereum repository on Github lists over 11K commits and 440 contributors and continues to grow.[63] Anecdotally, ethereum continues to host many emerging projects across a host of applications, including stablecoins, games, prediction markets, and decentralized finance. According to State of the DApps, projects such as Gnosis, Status, Trust Wallet, and Aragon have seen the most developer activity in the past 30 days.[64]

Initial coin offerings (ICOs) also serve as a relevant proxy to the growth of ethereum network adoption. Aside from the ethereum ERC-20 token standard serving as a highly efficient mechanism for crowdfunding campaigns, ICO volumes directionally signal development resources applied towards applications leveraging the ethereum network. While some of these projects will ultimately deploy their own blockchain separate from the ethereum network, the number of projects that have conducted ICOs generously skews in favor of the ethereum network. Though market demand has chilled for ICOs, many projects conceived during the boom cycle of 2017-2018 continue to operate today.

Figure 6 : Monthly ICO volume



Source: Coinschedule.com

Figure 7 : Quarterly ICO funding trend

Period	ICO Crowdsales	ICO Funding	Cumulative ICO Funding
1Q 2016	2	$5,800,000	$5,800,000
2Q 2016	10	$20,692,532	$26,492,532
3Q 2016	10	$26,742,115	$53,234,647
4Q 2016	30	$40,688,094	$93,922,741
CY 2016	52	$93,922,741	$93,922,741
1Q 2017	21	$123,333,107	$217,255,848
2Q 2017	72	$1,043,594,002	$1,260,849,850
3Q 2017	130	$1,788,505,664	$3,049,355,514
4Q 2017	219	$3,494,538,969	$6,543,894,483
CY 2017	442	$6,449,971,742	$6,543,894,483
1Q 2018	316	$8,291,911,041	$14,835,805,524
2Q 2018	358	$8,985,425,851	$23,821,231,375
3Q 2018	208	$2,264,143,956	$26,085,375,331
4Q 2018	169	$1,544,444,566	$27,629,819,897
CY 2018	1,051	$21,085,925,414	$27,629,819,897
1Q 2019	77	$595,395,167	$28,225,215,064
2Q 2019	76	$323,563,689	$28,548,778,753
3Q 2019	47	$427,743,260	$28,976,522,013
4Q 2019	11	$92,435,560	$29,068,957,573
CY 2019	211	$1,439,137,676	$29,068,957,573

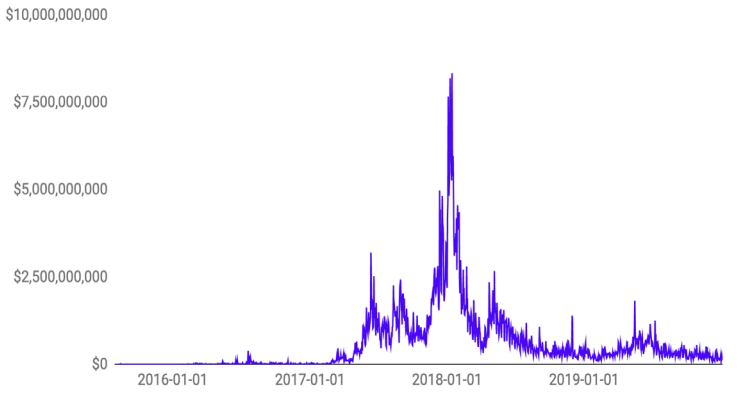
Source: Coinschedule.com

63 Ethereum Github Repository (https://github.com/ethereum/go-ethereum)

64 Dapp Statistics (https://www.stateofthedapps.com/rankings?sort=dev_30d&order=desc)

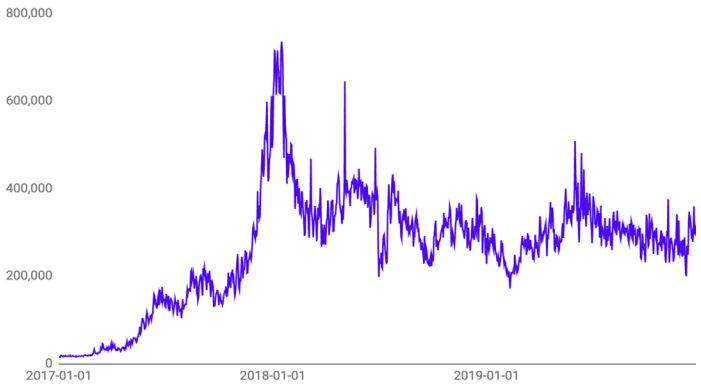
We can also consider daily on-chain volume and active users to gain a more holistic picture of user adoption and utilization of the network. As per figure 8, ethereum's daily on-chain volume hit an all-time high in January 2018, but sharply trended downwards for the rest of the year, stabilizing into 2019. This pattern indicates that network adoption largely followed market price trends. Daily active user count on the ethereum network has been seeing a steady decline as seen in figure 10, falling over 76% from its peak in January 2018 to February 2019 when active user count resumed growth. The network has seen continuous growth since February 2019, recording over 229K active daily users as of early-January 2020.[65]

Figure 8: Daily on-chain volume



Source: Coinmetrics.io

Figure 9: Daily active users



Source: Coinmetrics.io

Ethereum was once heralded as the alternative to bitcoin that would change the future of crypto by pioneering mainstream adoption with its distinct capabilities to support the expansion of blockchain usage. Ironically, its success as a smart contract platform and subsequent failures to scale spawned its own field of direct competitors. Though it still remains the leader in smart contract platforms in terms of market capitalization, its dominance has not gone unchallenged. Various projects rivaling ethereum were created to improve on the limitations of the platform, as outlined in figure 10.

Figure 10: Top competitors

Platform	Description	Similarities	Differences
EOS (EOS)	Platform for decentralized applications	Supports smart contracts Supports decentralized applications	Delegated Proof-of-Stake (DPoS) No tx fees; 1% inflation rate tied into native token, distributed to node holders
Stellar (XLM)	Platform for cross-border payments	Supports smart contracts	Proof-of-Stake (PoS) Low tx fees Smart contracts not Turing-complete In-house decentralized exchange
Cardano (ADA)	Platform for decentralized applications	Supports smart contracts	Proof-of-Stake (PoS) Two-layer platform
NEO (NEO)	Platform to digitize assets and automate management of digital assets using smart contracts	Supports smart contracts Supports decentralized applications	Proof-of-Stake (PoS) PKI (essential public infrastructure) used to verify identities Supports atomic swaps
Tron (TRX)	Platform for decentralized applications	Supports smart contracts Supports straight-forward contracts Supports Java programming language	Proof-of-Stake (PoS) Low - no tx fees Supports atomic swaps Adheres to Google Protobuf protocol for scaling Three-layer platform
Cosmos (ATOM)	Central platform which allows blockchains to exist in parallel, scale, and transfer value to one another	Supports independent blockchains	Bonded Proof-of-Stake (BPoS) Connects blockchains using Inter-Blockchain Communication (IBC)
Polkadot (DOT)	Central platform which allows transfer of data between private and public blockchains	Supports independent blockchains	Mainnet yet to launch

Source: Kraken Intelligence, project websites

65 Ethereum Network Statistics (coinmetrics.io)

According to DappRadar, almost 60% of dapps listed run on the ethereum network, 17% on EOS, followed by 17% on tron.[66] However, looking at the top 10 new dapp releases as of January 6, 2020, the ethereum and tron network each accounted for 40% of the new releases. Going forward, any changes in network dominance may be driven by the need for speed and scalability, the two current limitations of the ethereum network.

66 Dapp Statistics (https://dappradar.com/rankings)

VI. Conclusion

The ethereum network has experienced explosive growth in its five short years of operation. The application of smart contracts revolutionized the way we structure businesses and the continued technological developments of the network point to a future with boundless growth. However, while witnessing its many successes, we also uncovered many of its vulnerabilities. Despite ongoing improvement and patchwork, the network continues to see attacks on its platform, technological difficulties in deploying new infrastructure, and issues with scalability. Various competitors have come to the fore declaring themselves at par with ethereum, showcasing roadmaps that will overcome the shortcomings and complexities of this network. Regardless of this noise, however, ethereum treads on. Its developers and founders continue to work tirelessly on improving the platform and expanding its infrastructure while flexibly adjusting to unforeseen issues as they rise.

The network's ultimate goal of building ethereum 2.0 is an inspiring, but complex, future. It will tackle many of the issues we have witnessed, such as scalability, but the network will need to stay agile in dealing with the new attack vectors created by the complexities of ethereum 2.0. However, aside from the technological aspects of the network, we believe the societal values ethereum embodies will continue to be its strength. By promising a censorship-resistant, shared societal structure that defies current plutocratic arrangements, we see liberated access to finance and a progressive future in which ideals, like democracy, can be programmed through the use of dapps. The road is far and long for ethereum to reach its full potential, but if irresponsible, inflationary monetary activities, centralized data collection, and government censorship continues, the world may soon be ready to accept a truly global, decentralized computing platform.

Disclosure appendix

The information in this report is provided by, and is the sole opinion of, Kraken's research desk. The information is provided as general market commentary and should not be the basis for making investment decisions or be construed as investment advice with respect to any digital asset or the issuers thereof. Trading digital assets involves significant risk. Any person considering trading digital assets should seek independent advice on the suitability of any particular digital asset. Kraken does not guarantee the accuracy or completeness of the information provided in this report, does not control, endorse or adopt any third party content, and accepts no liability of any kind arising from the use of any information contained in the report, including without limitation, any loss of profit. Kraken expressly disclaims all warranties of accuracy, completeness, merchantability or fitness for a particular purpose with respect to the information in this report. Kraken shall not be responsible for any risks associated with accessing third party websites, including the use of hyperlinks. All market prices, data and other information are based upon selected public market data, reflect prevailing conditions, and research's views as of this date, all of which are subject to change without notice. This report has not been prepared in accordance with the legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research. Kraken and its affiliates hold positions in digital assets and may now or in the future hold a position in the subject of this research. This report is not directed or intended for distribution to, or use by, any person or entity who is a citizen or resident of, or located in a jurisdiction where such distribution or use would be contrary to applicable law or that would subject Kraken and/or its affiliates to any registration or licensing requirement. The digital assets described herein may or may not be eligible for sale in all jurisdictions.