Crypto Allocation

01.20.2022

George Dinenis[1]

Gerardo Lemus[2]

[1] george.dinenis@lamat-qanil.com
[2] gerardo.lemus@lamat-qanil.com, Lamat Qanil www.lamatuk.com





Motivation **3**
What are crypto assets and how do we value them? 3
Ecosystem explosive growth ? 4
What should be the allocation to crypto currencies ? 6

Background **7**
Simplified Blockchain model 7
Crypto Governance (Developers) 8
Decentralized ledger 9
Smart contracts 9
Validators 10
Tokens 10
Famous networks 10
Intrinsic Value 11
Crypto applications 12
Crypto Staking 12
Crypto as a store of value 12
Market abuse: Speculative measures 13
Crypto tokens to real life and vice versa 14
Naive financial comparators 15
Digital Gold market capitalization 15
VISA network market cap 16
Token as Fixed Income 16
DeFI tokens 17
Regulation 17
Valuation models (base token) 18
Application Valuation 18
Financial Scorecard 19

Crypto Valuation Factors **21**
Supply 21
Supply architecture 21
Whales 21
Demand 24
Retail Investors and Sentiment (Meme) 25
Institutional Investors 25
Applications 25
Stablecoins 26
Central Bank Digital Currencies 26
Decentralized Exchanges (DEX) and Decentralized Finance (DEFI) 27
Entertainment 27





Software Developers 28
Green Crypto, ESG 28
Environmental 28
Social 29
Governance 29
Fourth Estate 31
Validator Economics 31
Maximum Extractable Value 32

Crypto valuation model 33
Absolute Value 33
Relative Value 34

Case Study: Ethereum Valuation 36
Factors 37
Supply 37
London Fork Miner Reward Economics 39
Ethereum 2.0 Merge 41
Whales 43
Demand 43
Fat Protocol Theory 43
Retail Investors 44
Institutional Investors (regulated) 45
Institutional Investors (unregulated) 46
CBDC 46
Decentralized Applications 47
Network Effects / Development communities 48
Layer 2 Protocols 49
Validator Economics 53
Yield 53
ESG 54
Environmental 54
Social 54
Governance 55
Fourth Estate 56
Ethereum Technical Outlook 57
Proof of Stake Explained 58
PoS Smart Contract Platforms 59
Ecosystem Revenue 60

References 62
Online 62
Introductory books 62





Motivation

We develop a data driven framework for crypto currency[3] valuation, supporting a more transparent and efficient crypto market.

Our work aims to fill gaps and push the frontier of empirically based quantitative knowledge and information in an industry that has historically been characterized by hype and speculation in place of fundamentals.

What are crypto assets and how do we value them?

Investor focus is on Web 3 and the protocols that will facilitate the distributed ownership of 'internet of value'.

Crypto has primarily been used as a vehicle for speculation as buyers prioritize hoarding them while we wait for the killer app which will drive widespread need for crypto; but now the trend is changing. More crypto users are interacting with decentralised applications (which require the users to hold small amounts of crypto) and driving organic demand.

Cryptos are the asset used to reward the developers involved in the design, creation and maintenance of the crypto networks and applications.

Web 2 was not good at transferring incentives to open source projects (e.g. look at Wikipedia - which despite its iconic nature periodically requires external donations). Blockchain technology has shown that some open source platforms (such as Bitcoin and Ethereum) can be self funded (and profitable). As the projects/network grows, the value of these assets increases, incentivising network participants to continue to contribute.

Decentralised ownership of applications have significant advantages over centralised networks:

- If code can make strong commitments, you don't need central platforms to make and enforce the rules.
- Centralised platforms create economic drag as they morph into rent-extracting monopolies when there is weak regulation.
- Decentralised platforms allow creators, developers and consumers to share more of the profits than previously captured by centralised platforms.

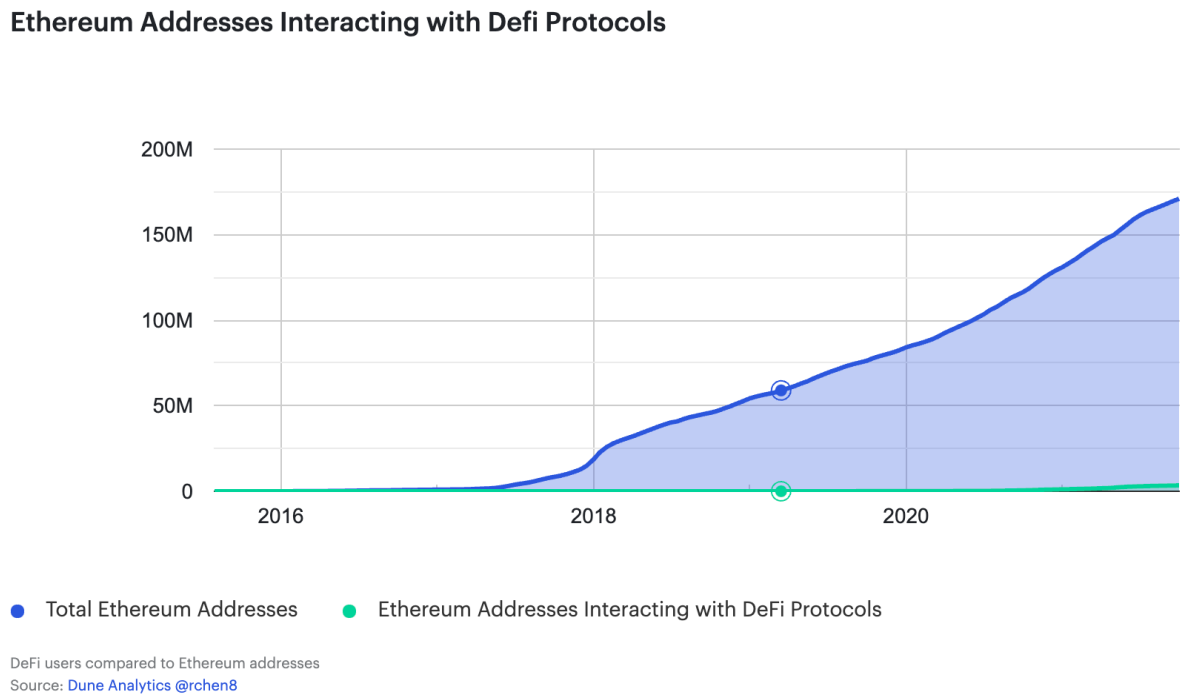
[3] We will be shortening cryptocurrency to *crypto* as it is now the common usage.

Ecosystem explosive growth ?

There are around 180 million unique Ethereum addresses according to Etherscan.io, the Ethereum blockchain explorer. Currently only a small but very rapidly growing segment of investors interact with Web 3.

Metamask, the most popular software wallet for interacting with the Ethereum ecosystem, last reported 21 million active users in November, up from 10 million in August and 5 million in April. Metamask is a gateway to web 3, and allows users to put ETH tokens to use in gaming, decentralised finance and purchasing and creating NFTs.

This 420% growth in seven months demonstrates the flow of users willing to use dApps. Unique Ethereum addresses have only grown from around 140 million to 180 million, or roughly 30% in the same period.



Likewise, the Phantom wallet, the gateway to the Solana ecosystem, is younger and growing more aggressively. They reported passing 1 million users on Nov 7th, just over a month after reporting passing the 500,000 user mark.

Investor sentiment and speculation has been the primary driver of crypto asset valuations so far, although using rigorous analysis it is possible to uncover opportunities on a relative-value basis. Data driven valuation frameworks allow us to compare blockchains and quantify and score characteristics under a set of assumptions.

More crucially, a rigorous framework helps investors separate the good from the bad in crypto.

A simplified[4] model of the crypto universe divides assets into two categories:

- **Decentralised Applications (L2) :** Exchanges, DeFi, Gaming etc.
- **Blockchains (L1) :** Ethereum, Solana, Algorand etc.

We begin with some simple definitions that will help us consider crypto in the context of financial assets.

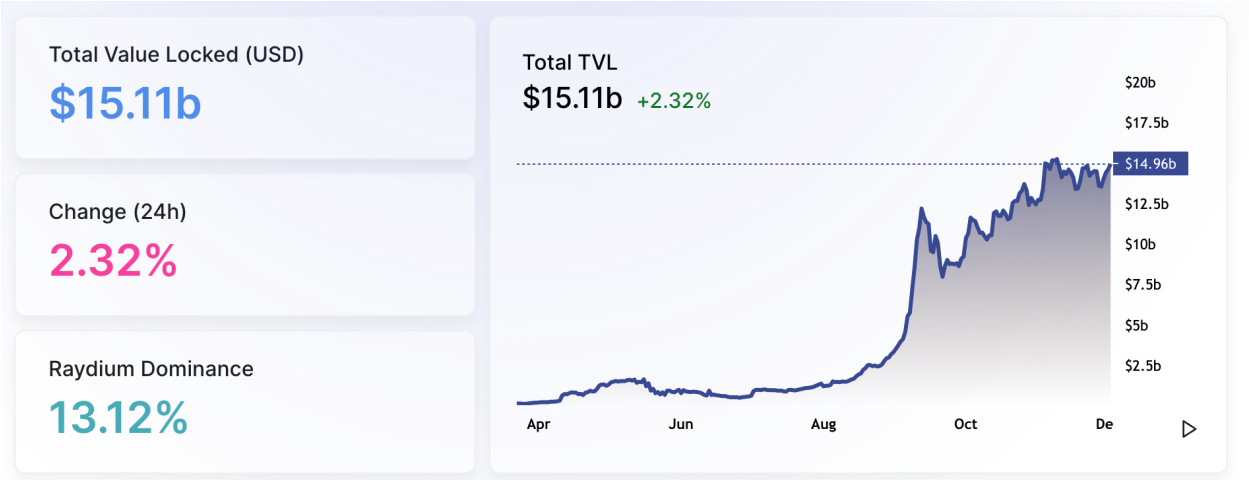
- Crypto assets are[5] a medium of storing and transferring value between network participants.
- Most Protocols[6] are distributed open-source systems that use in-protocol tokens to incentivise participants to maintain and grow the network.

Ethereum



[4] Simplified, as there are layer 2 blockchains designed and developed on top of layer 1 ones in order to solve scalability issues - such as Lightning networks on top of Bitcoin and Ethereum
[5] Cryptocurrencies can have additional characteristics, e.g. as unit of account - but to simplify the modelling we will overlook them for the moment.
[6] We will use the term *Network* as synonymous to protocol - but here is the formal definition: https://www.coinbase.com/learn/crypto-basics/what-is-a-protocol

Solana



What should be the allocation to crypto currencies ?

If you believe Economists like Roubini[7] or Hanke[8], crypto currencies have no place in the portfolios of investors. On the other hand, the Yale endowment[9] has famously increased the allocation to 'nontraditional asset classes' to improve diversification and returns - could crypto currencies be a legitimate nontraditional asset class ?

The market capitalization of the cryptocurrency market is estimated to be around $1.9 trillion[10], still a fraction of Gold ($11.5 trillion[11]) but no longer a rounding error. Gold-bugs have recommended[12] allocating between 2 to 10% of capital on the average pension fund portfolio.

The price of crypto currencies follows the same rules as any other asset: supply and demand. As the new technologies have been spearheaded by computer scientists, a communication chasm between traditionally educated financial analysts and the crypto community has been opened, our goal is to link both pool of experts by presenting the crypto ecosystem from the supply and demand perspective, including financial criteria such

---

7 https://www.theguardian.com/business/2021/mar/03/bitcoin-and-robinhood-will-end-badly-for-those-who-can-least-afford-it

8 https://www.bloomberg.com/news/articles/2021-03-09/bitcoin-has-zero-intrinsic-value-some-people-are-ok-with-that

9 https://investments.yale.edu/about-the-yio/

10 https://www.tradingview.com/markets/cryptocurrencies/global-charts/

11 https://finasko.com/gold-market-cap/

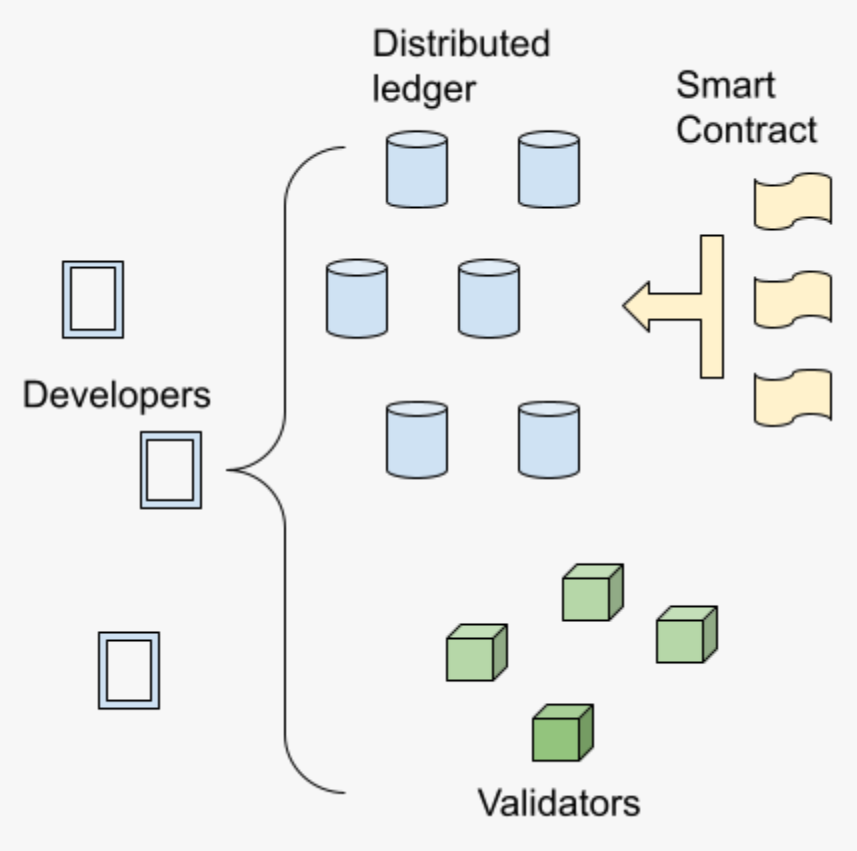
12 https://www.gold.org/goldhub/research/relevance-of-gold-as-a-strategic-asset-2019

as Environmental Social and Governance (ESG) and impact of future Government Regulations.

Background

We do not plan to fully describe how blockchain works (we recommend the documents and books set in the References), instead, we will review the basic value components of any asset and link them to the cryptocurrency ecosystem.

Simplified Blockchain model



A crypto currency ecosystem (CCE, also known as **chain** or **network**) consists of a **decentralized ledger** with **smart contract** capabilities that is maintained by **validators**. The validators receive **tokens** (also named crypto currency) as payment for their maintenance work, which they might exchange for fiat currency in the real world. The CCE

developers designed the software architecture and are in charge of upgrading it. In the real world the community of developers might choose to be organized under different organizational structures, and might have embedded in the CCE payments for further software work.

The decentralized ledger is used by users to record different kind of transactions, from network token movements to digital data storage; for each record they need to pay a transaction fee to the network (which has predefined rules to share it among developers and validators)

Crypto Governance (Developers)

Each cryptocurrency ecosystem is designed by a group of developers who need to decide (among other things):

- Network architecture (solving the 'double spend' issue, cryptography used, public, private or secret ledgers, etc.)
- Token supply dynamics (fixed or variable) ?
- How will validators be incentivized ? Using proof of work, proof of stake, other systems ?
- How will the virtual machine work ? Turing complete, incomplete, or adding loop costs ?
- How to solve the crypto trilemma ? (security, scalability and decentralization)

The trilemma refers to the inability of the initial crypto ecosystems to be secure, scalable and decentralized at the same time. Initially it was thought that the architects needed to pick up two characteristics and sacrifice the third (most often, scalability).

A common criticism of the original networks was their inability to replicate Visa's fabled 24k transactions per second[13]. Several solutions arose to fix scalability:

- Sacrificing decentralization (private chains, BSC[14] using a smaller set of validators),
- Sharding the network (partition the network to reduce the amount of information each node needs to process[15]: Ethereum[16]),

[13] https://news.bitcoin.com/no-visa-doesnt-handle-24000-tps-and-neither-does-your-pet-blockchain/
[14] https://wiki.rugdoc.io/docs/intro-to-bsc-binance-smart-chain/
[15] https://www.computerworld.com/article/3336187/sharding-what-it-is-and-why-so-many-blockchain-protocols-rely-on-it.html
[16] https://ethereum.org/en/eth2/shard-chains/





- Layer 2 networks[17] have been developed which use the original network as the backbone (but decrease transaction transparency and introduce extra complexity which might have unforeseen consequences).
- Fully designed networks incorporate scalable designs (Solana, Algorand)

The **crypto** prefix comes from the use "strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership"[18], but it is often confused with user anonymity. The incoming use of quantum computers to break cryptography systems will require serious upgrades by the developers.

Ongoing update of the ecosystem requires that there is a real life organization managing the upgrades. They can range from fully centralized and for profit organizations to fully open source and not for profit.

Decentralized ledger

Blockchain technology - for a good overview refer to the References section.

The developers can decide to make the ledger:

- Public, so that anyone can access it and read all the transaction data,
- Private, only readable by a limited number of users,
- Secret, which encrypts details of the transaction.

Government regulations will very likely have a strong impact on the ledger design; secret networks (like Monero)[19] seem to be very active on the dark web.

Smart contracts

Despite the legal sounding name, smart contracts are just software programs that can make additional records on the ledgers and do not constitute a legal contract enforceable in a jurisdiction. They run in virtual machines in the same maintenance infrastructure as the ledger validators (see below).

Languages to translate instructions into the virtual machine world tend to be targeted to each blockchain, and as a critical mass of developers is established on a blockchain there is a significant increase in the number of applications developed on it. Turing complete virtual machines can be used for more complex applications, but suffer from the curse of infinite loops (another reason why developers prefer to work in established languages and

[17] https://polygon.technology/
[18] https://en.wikipedia.org/wiki/Cryptocurrency
[19] https://www.newsbtc.com/news/bitcoin/why-the-dark-nets-most-active-market-ditched-bitcoin-for-monero/





blockchains as the code tends to be seen by many different eyes, reducing the amount of bugs).

Some of the most influential smart contracts (the basis for stable coins) is Ethereum's ERC20[20] and ERC721[21] (for non fungible tokens - NFT). See Applications for more details.

Validators

The validators[22] are incentivized to store the ledger, add new records and run the smart contracts with tokens. Depending on the architecture defined by the original developers, the capital cost of the required technological infrastructure can be very high.

Tokens

Each network has its own token[23] that is used to pay the validators (and in some cases, the developers) on their wallet address.

Non-validators can create their own wallet address and exchange real life assets against someone who holds the token in a real life transaction, but the transfer of the real life asset remains one between two trusted counterparties.

If party A sends the token to party B but party B refuses to reciprocate with the real life asset, the case has to be settled in real life using real life law jurisdiction. To alleviate this issue, centralized crypto exchanges have arisen which will necessarily be regulated by the government given the real life implications.

Network (or chain) tokens should not be confused with smart contract derived fungible tokens (which colloquially also tend to be called 'crypto') which run on top of a network but have extended applications (more in Yield per token)

Famous networks

The Bitcoin network was the very first successful CCE. The original developer was the infamous Satoshi Nakamoto[24], but it is now an open source project[25] that can be improved by anyone as long as the changes are adopted by most of the users. Satoshi selected proof of work as the method to select which one of the validators would receive the bitcoin as the token, and the original developers had 'first mover' advantage to start running as validators. Smart contracts were included in the original design, but they were deprecated

[20] https://ethereum.org/en/developers/docs/standards/tokens/erc-20/
[21] https://101blockchains.com/erc20-vs-erc721/
[22] We keep use the term validator as an umbrella term to encompass both proof of work **miners** and proof of stake validators.
[23] Token and crypto are terms used as synonymous.
[24] https://bitcoin.org/bitcoin.pdf Bitcoin: A Peer-to-Peer Electronic Cash System
[25] https://bitcoin.org/en/faq#who-controls-the-bitcoin-network





to be ‘non Turing complete’, meaning that they are assured to always end in a finite amount of time (to avoid infinite loops which can cripple the network).

Ethereum has a similar open source philosophy, but the original developers (like Vitalik Buterin) still have an outsized influence on the direction of the software upgrading. The vital difference was to include ‘Turing complete’ smart contracts to be, which allows for very sophisticated applications to be developed.

The open source code nature permits anyone to create a new ecosystem, and browsing the internet certainly shows it. Dogecoin was built as a joke[26] by cloning Litecoin (also based on Bitcoin), but now has become an irreverent store of value.

Intrinsic Value

In the words of Roubini[27]:

> *"What's an asset? Usually, it gives you some income or cash flow. Stocks give you dividends. Bonds give you a coupon. Loans give you interest," he said. "Now, gold doesn't have income but it has uses in industry. It has utility because it has uses in jewelry for thousands of years. It has been a stable store of value whenever there is inflation or deflation."*

Any asset is supposed to have an intrinsic value which depends on different factors:

- How do you use the asset ? Commodities such as timber can be used in many industries. This is one of the most misunderstood factors in cryptocurrencies; several economists argue that there is no intrinsic value as they do not understand where the cryptos are used. Crypto applications.
- Does the asset give you expected cash flows ? Equities and fixed income assets are valued based on the net present value of the expected cash flows. Parts of the crypto ecosystem now also provide future cash flows - but as such they will most likely become regulated. Crypto Staking.
- Is the asset a store of value ? Gold has some industry value, but arguably the factor driving its price is the belief that it is a *stable* store of value. Most of the critiques of economists against cryptocurrencies target the stability by highlighting *speculative* factors surrounding the chains. Crypto as a store of value.

---

26 https://www.bloomberg.com/news/articles/2021-02-11/dogecoin-s-creator-is-just-as-baffled-as-you-are-about-its-rise

27 https://www.kitco.com/news/2021-05-10/Bitcoin-will-never-be-digital-gold-and-Central-Bank-Digital-Currencies-will-kill-cryptos-Roubini.html





Crypto applications

The most basic use in a crypto currency ecosystem is the recording of a crypto transaction into a decentralized ledger that so far has proved to be impervious to hacking or government control. Notice that we mean the ledger itself is the permanent set of records - there have been cases of the new records being added without the agreement of all the parties (e.g. hacking of accounts and transferring crypto value from one wallet to another) as well as cases of the permanent record being rewritten when a majority of stakeholders agree (see the Ether hard fork case[28]). In both cases, the final record remains.

Applications where companies are required to save the data in a safe place are quite common:

- Imagine saving all of the UK Companies House database into a crypto blockchain that is public instead of using a centralized database stored in an Amazon server - the intrinsic value for the Companies House developers would be the cost of replacing the centralized database into a blockchain.
- Imagine allowing the use of the smart contract to allow for automated market makers in foreign exchange markets: each transaction is recorded in the ledger while using the smart contract capability inherent in some crypto ecosystems[29]. The intrinsic value would be the cost of replacing the current FX market maker facilities and back office.

Crypto Staking

Bitcoin, the first cryptocurrency, was designed to resemble 'digital gold' (link), and has been classified as a commodity by the CFTC[30] [31]. It has a limited supply, and holding it does not provide any rights to future cash flows. However, multiple new crypto ecosystems have been developed (usually based proof of stake) which give the holder the right to receive future crypto flows. (More details on Yield per token)

Crypto as a store of value

Most of the controversy and debates from economists surround the 'stable store of value' use of the crypto ecosystem.

---

[28] https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/
[29] https://arxiv.org/pdf/2109.12196.pdf Automated Market-Making for Fiat Currencies
[30] https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/oceo_bitcoinbasics0218.pdf
[31] https://www.congress.gov/bill/116th-congress/house-bill/2144/text?q=%7B%22search%22%3A%5B%22%5C%22token+taxonomy+act%5C%22%22%5D%7D&r=1&s=10





Lets recap:

- The basic use of the crypto ecosystem is to store records in a decentralized ledger.
- The incentive for 'ecosystem maintainers' to save and update the ledger is by being paid in tokens (the payment being registered in the same ledger)
- The tokens need to be redeemed in a fiat currency to be able to pay for the underlying computer power.

Unsurprisingly, economists that do not understand the basic use of the ledger argue on the circularity of the crypto ecosystem: if there is no other use rather than recording the own crypto transactions, why use the ecosystem at all ?

The store of value is initially derived from the hope of the validators that someone else is willing to pay them for maintaining the networks, and this hope should increase once there are useful applications of the network. If no bona fide users need the token to pay for record storage, the price should fall.

Non fungible tokens (NFT) are an extreme example of the 'store of value' argument - the price of a token being the value that two parties are willing to transact.

Dogecoin, a coin designed without any (initial) utility[32], is an extreme case of a pure store of value, and can be used to monitor bubble behaviour driven by **speculative** factors.

Market abuse: Speculative measures

Regulated financial markets have identified and made illegal market manipulation techniques[33]:

> *"(3)* ***pump and dump*** *– that is, taking a long position in a qualifying investment and then disseminating misleading positive information about the qualifying investment with a view to increasing its price;*
>
> *(4)* ***trash and cash*** *– that is, taking a short position in a qualifying investment and then disseminating misleading negative information about the qualifying investment, with a view to driving down its price."*

32 https://www.barrons.com/articles/dogecoin-started-as-a-joke-now-its-too-important-to-laugh-off-51620229273

33 https://www.planetcompliance.com/the-7-deadly-sins-of-market-abuse-part-v-manipulating-devices/





Speculative attacks distort the price setting mechanism[34]; the unregulated nature of the crypto markets removes buyer protection (in effect imposing *caveat emptor*[35]) and forces the buyer to perform due diligence[36].

Market manipulation can be measured on public ledgers by applying the same techniques as regulators: identify insiders and their trades before public announcements, identify attempts to pump and dump by monitoring social networks and transactions (as in the academic article that exposed Tether/Binance collusion to maintain the price of Bitcoin in 2017 *"Is Bitcoin Really Untethered?"*[37])

Crypto tokens to real life and vice versa

The *magic* of crypto currency networks arose when a fiat to token market was created. Exchanging tokens for real life assets allows developers to pay for their real life needs (food, shelter, equipment and energy for example).

Validators and developers receive their crypto tokens by:

- Exchanging intellectual property, and software development for tokens,
- Exchanging the use of technological tools (servers) and energy for tokens.

Transferring crypto assets to real life requires a counterparty that is willing to transfer real life currencies or other assets in exchange for a transaction. The record of such transaction might be stored in a blockchain, but its **enforcement** remains a real life issue:

- Peer to peer transactions needs to be done between trusted parties (for example, the very first bitcoin to USD transaction is easily verifiable in the blockchain[38] but the fiat currency was done as a private Paypal transaction).
- Centralized exchanges need to be trusted (remember Mount Gox[39]).
- NFTs linked to real life assets still need to be covered by a legal contract[40] (nothing to do with the smart contract).

All of these issues will eventually be covered by **regulations** of different countries.

---

[34] https://en.wikipedia.org/wiki/Market_abuse

[35] https://www.investopedia.com/terms/c/caveatemptor.asp
[36] https://en.wikipedia.org/wiki/Due_diligence
[37] https://onlinelibrary.wiley.com/doi/full/10.1111/jofi.12903
[38] https://www.blockchain.com/en/btc/tx/7dff938918f07619abd38e4510890396b1cef4fbeca154fb7aafba8843295ea2
[39] https://en.wikipedia.org/wiki/Mt._Gox
[40] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3928901 "The property Law of Tokens"

Naive financial comparators

The desire to explain crypto currency ecosystems to the general public tends to exploit similes such as:

- Bitcoin is like digital gold (just google it)
- Ethereum will be like a decentralized VISA network[41] once it reaches the same capability of transactions per second

Unfortunately, there is a tendency to keep pushing the simile to equate value propositions:

- If Bitcoin is like gold, and gold is worth $11tn, then Bitcoin can easily reach USD500k (roughly $11tn divided by 21mn)
- If Ethereum is like VISA (market capitalization of $500bn), it can still increase 30% from its current market capitalization of $388bn after Ethereum 2.0 is launched

Both assertions are wrong:

Digital Gold market capitalization

> *"A store of value is any commodity or asset that would normally retain purchasing power **into the future**"*[42]

Bitcoin has been classified as a commodity by the CFTC, **but** it should be valuable today as long as it can be exchanged not only for a short term but at any time in the future (like gold, even **after** we are dead).

Gold has existed as a store of value for many (not all[43]) civilizations and given its chemical properties will remain stable for many years to come, but bitcoin will require a fully functioning validator networks (servers, computers and energy) as well as constant upgrades by a dedicated group of developers (remember, the current crypto technology used by Bitcoin might be obsolete in the next ten years[44] without significant code upgrades). In 2140 after the last bitcoin is mined, the remaining incentives for validators will be the network fees, required for transactions; it is not clear if by then the costs to sustain the network will be covered by those fees.

---

[41] https://www.tbstat.com/wp/uploads/2021/09/Ethereum-investor-guide.pdf
[42] https://en.wikipedia.org/wiki/Store_of_value
[43] https://www.reddit.com/r/AskHistorians/comments/4n657j/comment/d41n8sq/?utm_source=share&utm_medium=web2x&context=3 "How much value did the Aztecs place on gold in Pre-Conquest Mexico?"
[44] https://www.cnbc.com/2021/06/10/long-term-crypto-threat-quantum-computers-hacking-bitcoin-wallets.html





We highly recommend reading Erb's "Bitcoin is Exactly Like Gold Except When it Isn't"[45] which has considerably delved into the argument.

VISA network market cap

VISA (and Mastercard, etc) is a ***centralized*** ledger that profits[46] (among different revenue channels) from network fees and decided by the same corporation. In a decentralized chain, the network fees are defined (even capped) by the developers and ***shared*** by multiple validators.

VISA shares (a security) give the holders the **right** to future dividends (a stock price is the net present value of all future dividends) as well as legal claim of all the company assets after creditors under a specific legal jurisdiction, *but* are not used to run the network. Ethereum tokens at the moment (while using proof of work) only allow the use of the network (although it is planned in Ethereum 2.0 to return a network stake after proof of stake is implemented), *but* the profit sharing can be capped depending on the number of validators in the network, and do not provide legal claims to assets owned by the network. Also, the price of Ether includes a significant amount of *store of value* which is not existent for share prices.

As an extreme example: Algorand can decrease the transaction fee to negligible values by developer consensus while deciding on the *inflation* (the rate of additional tokens rewarded to the validators). The tradeoff is chosen to maximize the store of value element of a token.

The key point for Equity-like valuations will be the move to proof of stake, with the understanding that using Equity valuation tools does not imply they can be compared to existing equities.

Token as Fixed Income

Commodity crypto currencies like Bitcoin do not provide any right to receive further token flows. However:

- Proof of stake networks can return a periodic yield for tokens that are **staked** i.e. stored by a validator to gain the right be compensated for maintaining the network (see details on Proof of Stake Explained)[47] [48]. As the yield is generated as part of the architecture, the yield can be considered almost **risk free** (within the chain base and for honest and reliable validators).

[45] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3746997
[46] https://www.investopedia.com/how-visa-makes-money-4799098

[47] https://ethereumprice.org/eth-2-calculator/
[48] https://algoexplorer.io/rewards-calculator?





- DeFI can return a yield for tokens that are 'staked' in some of the dApps. However, the extra yield is the sharing of fees generated by the dApp protocol, which will entail different risks (capital is at risk in case of some adverse scenario). As the dApps become more complicated, the risk analysis is not straightforward.
- Centralized Finance, Peer to Peer or Securitized lending also offer yields with traditional credit risk attached (to the counterparty/ies)

The decentralized world decided to use the Fixed Income concept of yield, but we can apply Equity concepts to derive a value model to each token.

DeFI tokens

Smart contracts that run on a network tend to also use the nomenclature of 'token'. However it is necessary to pay the transaction fees on the network token in order to run the application.

Some of them (e.g. Automated Market Makers AMM) can provide a yield when the smart contract token (liquidity token) is staked, but the value of the liquidity token will be a function of the tokens being traded by the AMM (e.g., in a ETH-USDC AMM, the liquidity token will be a weighted average of the amounts used to provide liquidity). The yield returned is a portion of the fees charged by the AMM to outside traders.

Quantitative models evaluating the future token flows of this AMM can be derived, even as AMMs increase in complexity.

Regulation

The addition of yield introduces potential regulation minefields:

Just because Bitcoin is a commodity does not grandfather the status to all subsequent networks. The SEC uses the Howey test[49] to determine if an asset is a security or not:

> *"The test itself involves a series of four questions that need to be asked about the particular transaction. If the asset meets these criteria then it can be considered an investment contract.*
>
> - *It is an Investment of money*
> - *There is an expectation of profits from the investment*
> - *The money invested is in a common enterprise*
> - *Any profit comes from the efforts of a promoter of a third party"*[50]

[49] https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets
[50] https://www.coinbureau.com/analysis/howey-test-cryptocurrency/





If the asset is a security the SEC will regulate it as an investment, which has brought immediate consequences to some developers:

> *"Washington D.C., Dec. 22, 2020 —*
>
> *The Securities and Exchange Commission announced today that it has filed an action against Ripple Labs Inc. and two of its executives, who are also significant security holders, alleging that they raised over $1.3 billion through an unregistered, ongoing digital asset securities offering."*[51]

Security rules usually have investor protection priorities in mind, but will also have **tax** implications[52] [53].

Valuation models (base token)

The base token risk free rate should be easy to incorporate into valuation models using familiar Fixed Income net present value formulas (most of the complexity for network tokens should come from the exchange risk against fiat), unless there is a change of regulations regarding the taxation of tokens gained from yield.

Token network governance becomes a potential source of uncertainty which needs to be taken into account.

Application Valuation

To understand how to value the native tokens of smart contract platforms such as Ethereum, it is instructive to start with the valuation of applications. Valuation of applications is more straightforward as they are more equity-like, in the way traditional finance investors are familiar.

Uniswap is what is known as a DeFi protocol. It is a decentralised exchange[54].

Uniswap's token is known as a governance token; tokens are used to incentivise participants to do the open source work required for maintenance of the network, and are required to vote for changes in the structure of the application.

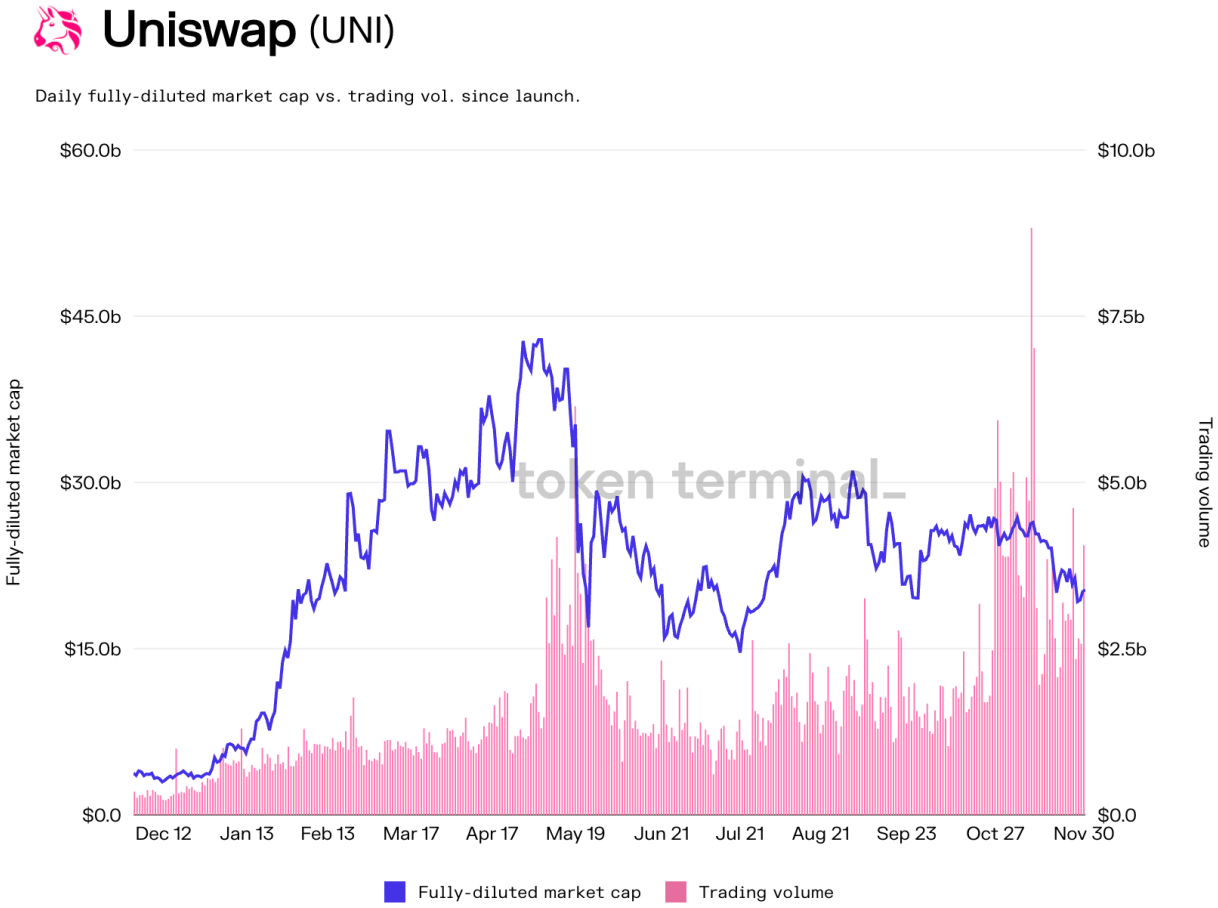
As adoption grows, the voting control becomes more valuable. The incentive to hold becomes more valuable as decisions that can impact the price of the token need to be made.

---

[51] https://www.sec.gov/news/press-release/2020-338
[52] https://www.gov.uk/government/publications/tax-on-cryptoassets
[53] https://www.cointracker.io/blog/defi-yield-farming-crypto-tax-guide
[54] https://messari.io/article/valuing-uniswap-the-world-s-largest-decentralized-exchange

Bitcoin demonstrated that this incentive system has been proven; co-existence of multiple interoperable blockchains could reduce the store of value of any single one but also make the overall system more resilient.

Transaction volume can be used as a proxy for valuing.



Financial Scorecard

Utility

Network effects / Demand:	
Users	User rate of growth
dApp	dApp token usage (number of transactions) dApp rate of growth (transaction growth)
dApp devs	Dev rate of growth (Github / Discord)

Token Flows	Validator economics	Direct rewards, indirect Maximum Extractable Value (MEV)[55] Expected changes Possible changes

Store of Value	Stable	Sticky user deposits (*hodlers [sic]*)
	Speculative	Insiders Whales Social influencers
	Governance (Developers)	Supply (inflation, direct rewards) Supply policy changes (expected, possible) Energy (PoW / PoS) Social (Money Laundering) Governance (Regulatory risks)

Initial approach:

Relative Valuation:

[55] https://explore.flashbots.net/





Assign relative scores within each factor ranking chains.

Forecast relative market cap share

Crypto Valuation Factors

We will describe qualitatively and quantitatively the crypto pricing factors that we have identified so far.

Supply

Token supply dynamics on any network is decided by the original set of developers, and have become a large factor in the pricing of some tokens.

Supply architecture

Developers decide (and can modify) the supply of the tokens. The most common examples are:

- **Fixed supply**. As its name suggests, a limited number of tokens and distribution plan over time is defined from day 0. The most famous is Bitcoin with its limit of 21millions bitcoins to be reached by 2140[56].
- **Infinite supply**. Fewer people are aware that some tokens **do not** have a token limit, nor a predefined growth rate. For example, the growth rate of ether is a function of other network factors (such as reward amount for each validated transaction) which can be changed by the open source community on a Ethereum Improvement Proposal (EIP[57]).
- **Decreasing supply**. It is possible to design tokens that have a decreasing supply (e.g. Southpole), although they seem to be gimmicky.

For short term applications the **circulating supply**[58] is very relevant as it defines the limit of tokens available to trade at the moment. Networks with fixed supply and deterministic token release should be fully priced in the market, but networks where the release of tokens is unclear might be penalized in case of unforeseen releases.

Token growth rate is an important factor on the supply analysis, which requires in depth understanding of the network architecture (monitoring open source forums directly, establishing direct communication with developer groups)

---

[56] https://en.wikipedia.org/wiki/Bitcoin#Supply
[57] https://github.com/ethereum/EIPs/issues/960
[58] https://coinguides.org/circulating-supply-total-supply-max-supply/

Whales

Circulating supply might give an erroneous view of token liquidity, especially if it is locked in the accounts of a few large accounts.

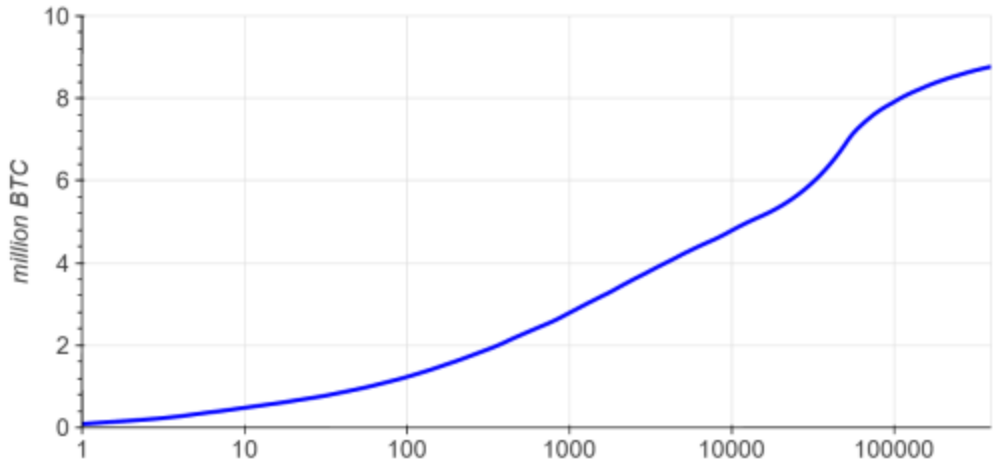
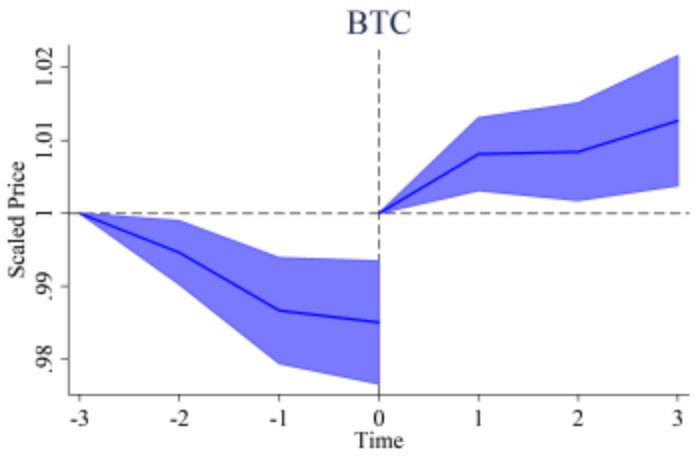


Figure 23: Ownership concentration of individual addresses. The figure shows the concentration of Bitcoin held by individual holders. We sort individual clusters according to their balance at the end of 2020, and plot their cumulative balance against the number of individual clusters that are holding these bitcoins.

The National Bureau of Economic Research published[59] the graph above implying that around 1000 individual holders control around 2.8 million BTC (almost 15% of the current circulating supply of 18.87mn[60]).

Numerous data sources[61] that analyze the location and the flows of whale accounts have appeared, and academic research has previously identified causaction between flows of some of these whales and token prices (in 2018 links were found between tether purchases and Bitcoin prices):

[59] Working Paper 29396 'BLOCKCHAIN ANALYSIS OF THE BITCOIN MARKET'
https://www.nber.org/system/files/working_papers/w29396/w29396.pdf
[60] https://coinguides.org/live-coin-watch/
[61] https://whale-alert.io/

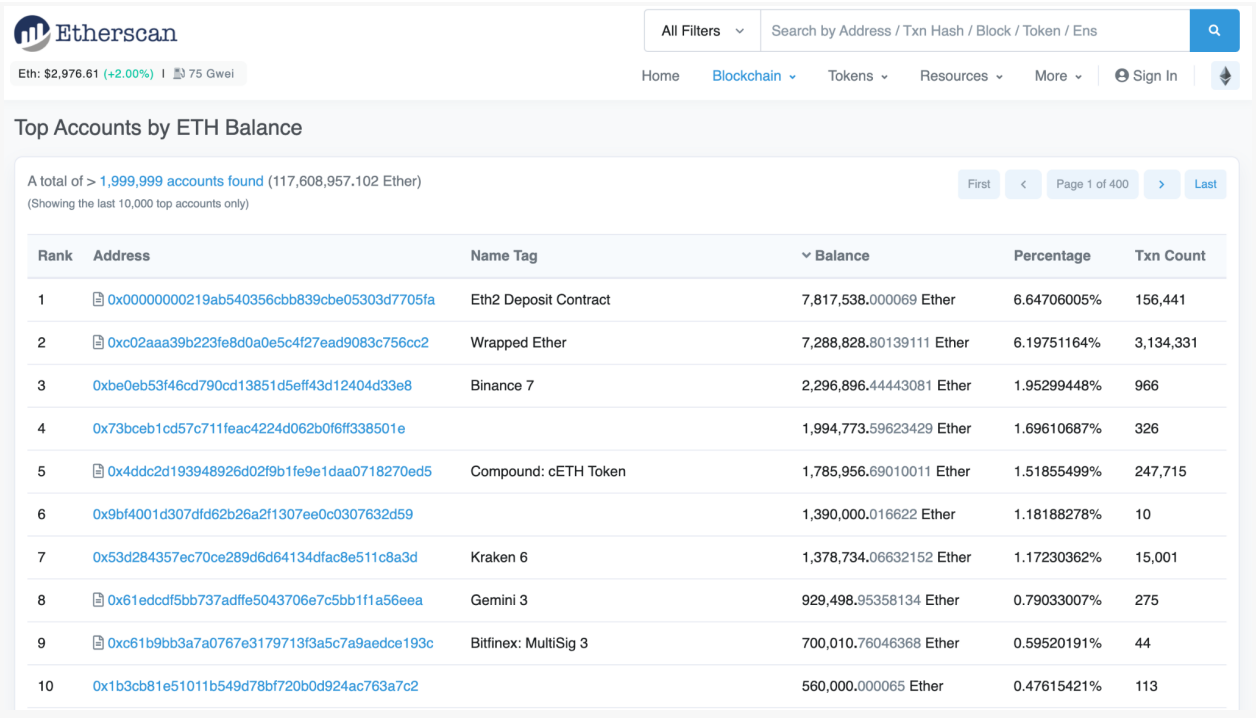


> *"Prices of Bitcoin ... around High 1LSg Flow Events. ... shows Bitcoin prices three hours before and after the top 1% of high 1LSg flow hours. Prices are scaled to one at time -3 before the event and at time zero after the event. Scaled prices are averaged across the events. The high 1LSg flows occur between time -1 and time 0 ..."* (graph from page 21[62])

Whale identification is possible for networks that have a public ledger, as it can be data mined. Networks that have a secret ledger (like Monero) were developed to sidestep this information, but are likely to have issues with Government regulations - Homeland Security has fomented the development of Blockchain Forensic Analytics[63].

[62] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066 Is Bitcoin Really Un-Tethered?

[63] https://www.dhs.gov/science-and-technology/news/2019/02/01/news-release-dhs-fy19-sbir-proposal-submission-extended



https://www.blockchain.com/explorer
https://blockexplorer.com/
https://github.com/citp/BlockSci
https://www.walletexplorer.com/
https://etherscan.io/accounts

Demand

While the network defines the supply dynamics, demand of tokens comes from various sources:

- Real life individual/institutions (who usually need to transact via a centralized exchanges[64]). Data from each exchange can be usually obtained via API (like Binance [65]).

[64] https://www.coingecko.com/en/exchanges
[65] https://docs.binance.org/api-reference/transactions.html

- Decentralized applications (dapps) usually need to pay a transaction fee in the token of the network to run. The exponential growth of dapps can drive the price paid per fee (particularly for unscalable networks) which might have a second order impact on the price of the token. Rankings[66]:

		CATEGORY	BALANCE	USERS	VOLUME	ACTIVITY
Ad	Use DAPRD for 125% 1st deposit bon ETH	Gambling	$0	0 –	$0	
1	Uniswap V3 ETH	DeFi	$3.31B	185.93k -11.70%	$54.82B	
2	Uniswap ETH	Exchanges	$8.57B	291.04k -12.22%	$39.76B	
3	Dfyn Network Polygon	Exchanges	$100.33	12.63k -31.19%	$25.12B	
4	PancakeSwap BSC	DeFi	$4B	3.06M +22.37%	$24.26B	
5	Compound ETH	DeFi	$6.21B	4.02k -8.73%	$15.38B	
6	Fei Protocol ETH	DeFi	$268.33M	1.7k +47.07%	$13.51B	
7	Sushi	DeFi	$3.9B	128.84k +3.30%	$13.11B	

- Cross network demand. New platforms are being developed to allow for token transactions between incompatible networks.

Metcalfe Law

> *"Metcalfe's Law is not a scientific law rather it is an aspirational assertion that started as a sales tool to pitch the potential of the internet (or more specifically of Ethernet). The idea is that the impact or value of a network can be thought of as being proportional to the square of the number of connected users. While it may be difficult to precisely define what a connected user is, the math is simple.*
>
> *Ten users would equal a network "value" of 100 and 1,000 users would equal a network "value"of 1,000,000."*[67]

Retail Investors and Sentiment (Meme)

Individuals started the transfer of fiat into tokens.

The 'store of value' factor is one the main driver of cryptocurrencies prices is, which is driven (or manipulated) by the belief of multiple users. It has been common for a small section of influencers (Elon Musk for example[68]) to be able to move the price of tokens with

[66] https://dappradar.com/rankings
[67] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3746997
[68] https://www.forbes.com/sites/ronshevlin/2021/02/21/how-elon-musk-moves-the-price-of-bitcoin-with-his-twitter-activity/





social media endorsements. Dogecoin is a prime case of pure 'store of value', hence the meme coin moniker.

Institutional Investors

Regulated and unregulated institutional investors can be monitored by following regulated markets (such as the CME[69] Bitcoin and Ether futures) as well as known wallet addresses of Centralized Exchanges. (see Whales above)

Applications

Decentralized applications (dapps) underpinning games, decentralized exchanges and decentralized finance (as the top categories) have famously exploded the use of some blockchains (particularly Ethereum) to the point of dramatically increasing the price per transaction[70] [71]. Users of the dapps need to purchase the network token to run them, fomenting solid demand for the token.

Some networks have designed extremely low fees in order to attract dapp development (e.g. Solana, Algorand), so demand metrics need to consider various elements such as:

- Transaction fee on token space,
- Growth of dapp ecosystem,
- Transaction per seconds limit

Stablecoins

Despite ending in -coin, they are 'real life' crypto applications built on top of existing networks using smart contracts. For example, USDC has been built (is supported) over multiple chains[72] including Ethereum, Algorand and Solana:

> *"USDC smart contract*
>
> *USDC is available as Ethereum ERC-20, Algorand ASA, Solana SPL, Stellar asset, and TRON TRC-20. Support and integrate the token smart contract with any Ethereum, Algorand, Solana, Stellar, and TRON applications."*[73] [74]

The amount of stablecoin issued in each chain can be used as a measure of its popularity and demand.

---

[69] https://www.cmegroup.com/markets/cryptocurrencies/bitcoin/bitcoin.quotes.html
[70] https://ethereumprice.org/gas/
[71] https://cryptobriefing.com/crypto-kitties-have-taken-over-ethereum-network-icos-canceling-2/
[72] https://www.circle.com/en/multichain-usdc
[73] https://www.circle.com/en/usdc
[74] https://www.centre.io/usdc-transparency USDC audits





It is very important to note that there is a high level of interest from multiple governments, and it is almost a certainty that they will become highly regulated[75].

Central Bank Digital Currencies

Digital currencies (not necessarily built on top of decentralized networks) are being studied by major central banks[76]:

> *A group of central banks, together with the Bank for International Settlements, are working together to explore central bank digital currencies (CBDCs) for the public ("general purpose" or "retail" CBDC).*[77]

One of the major applications envisaged are cross-border transfers[78] which potentially could use 'Distributed Ledger Technologies' (DLT).

Decentralized Exchanges (DEX) and Decentralized Finance (DEFI)

DEXs have become one of the most used dApps for several chains. A DEX uses smart contracts to become Automated Market Makers[79] that can be used to trade from one digital token to another within a chain.

Combined with available stablecoins, the use of DEXs tends to increase, providing a high amount of demand for the underlying chain token (which is needed to pay the transaction fees).

Entertainment

It is the highest profile use of smart contracts (as NFTs), and even Forbes[80] has published an article explaining it. Games (cryptokitties[81]), digital art NFT[82], etc. are available and ca be monitored in the underlying blockchain.
There is now a significant backlash against NFTs. There is the misconception that -in the case of digital art- the visual representation is stored in the blockchain and can only be used by the owner; in reality the current NFT contracts only store on the blockchain a link

[75] https://www.nytimes.com/2021/07/19/business/stablecoins-regulation.html
[76] https://www.financemagnates.com/cryptocurrency/news/french-and-swiss-central-banks-to-test-cross-border-cbdc-payments/
[77] CBDC BIS summary: https://www.bis.org/publ/othp42.pdf
[78] https://www.bis.org/publ/othp40.pdf
[79] https://uniswap.org/whitepaper-v3.pdf
[80] https://www.forbes.com/advisor/investing/nft-non-fungible-token/
[81] https://www.cryptokitties.co/
[82] https://www.nytimes.com/2021/07/23/your-money/nft-art-lebron-james-damien-hirst.html



to a url. There is huge legal uncertainty about ownership of the underlying digital (or real) asset[83]:

> *The NFT hype promises a new way of giving value to intangible assets.* ***As legal tokens, however, NFTs fail****. All legal tokens evolved as a solution to a problem. Negotiable instruments and certificated securities developed to give certainty to the transfer of intangible rights. Deeds of real property developed to prove the transfer of land, an asset that cannot be physically transferred. Bills of lading developed to facilitate transfers of goods in transit. Other "token-like" items such as automobile certificates of title and bailment tickets provide evidence of ownership.*
>
> ***NFTs****, however, are a solution in search of a problem. They* ***do not provide any link to an underlying asset****, and therefore do not facilitate the transfer of any asset. A blockchain, like a recording system, provides a record of ownership, but in the case of NFTs, all it provides is a record of who owns the NFT, not of who owns any reference asset.*

Despite unclear property rights, NFT transactions have driven the number of transactions in networks such as Ethereum (in December 2017 Cryptokitties drove the network transaction requests from 622k to 1.07mn[84]).

Software Developers

Many dApps are built by developers which initially follow open source platforms (such as public github repositories) and debate in gaming chat rooms (e.g. Discord). Electric Capital writes reports[85] about the growth of networks, and has developed a taxonomy to aid on the analysis of open source crypto ecosystems[86].

Green Crypto, ESG

Environmental, Social and Government concerns are at the forefront of many government and investors priorities.

Environmental

By now it is a common argument to decry the use of energy of Bitcoin (or other proof of work networks). The Cambridge Bitcoin Electricity Consumption Index[87] produces estimates

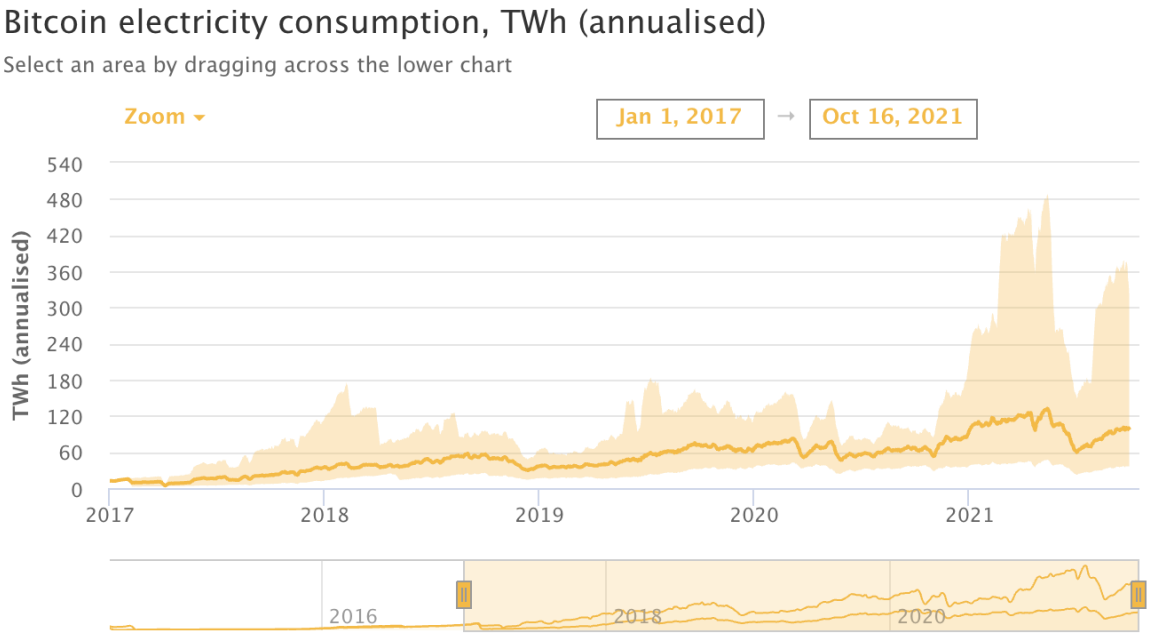
[83] The Property Law of Tokens by Juliet M. Moringiello, Christopher K. Odinet :: SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3928901
[84] https://gitcoin.co/blog/a-brief-history-of-gas-prices-on-ethereum/
[85] https://medium.com/electric-capital/electric-capital-developer-report-2020-9417165c6444
[86] https://github.com/electric-capital/crypto-ecosystems
[87] https://cbeci.org/

of the energy required to run the network, which necessarily has to increase when the price of Bitcoin increases.

There is a huge debate about the validity of the Cambridge Index, with Nic Carter arguing that[88]

> "***Bitcoin Can Use Energy That Other Industries Can't***
>
> *Another key factor that makes Bitcoin's energy consumption different from that of most other industries is that Bitcoin can be mined anywhere. Almost all of the energy used worldwide must be produced relatively close to its end users — but Bitcoin has no such limitation, enabling miners to utilize power sources that are inaccessible for most other applications."*

Despite those arguments, governments around the world have banned are are considering banning crypto mining [89] [90].



[88] https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume
[89] https://news.yahoo.com/china-bans-crypto-trading-mining-155020817.html
[90] https://www.msn.com/en-us/money/markets/top-eu-regulator-urges-e2-80-98ban-e2-80-99-on-crypto-mining-that-he-claims-is-sucking-up-renewable-energy/ar-AASVZRC?pfr=1





To alleviate this issue, proof of stake protocols have been developed, although there is also significant energy consumption[91].

Social

Uses of cryptocurrencies by criminal enterprises has been widely documented, albeit the public nature of most of the networks allows the tracking of illicit funds[92]. However, some networks that were designed with full privacy might end being on the wrong side of regulations if the authorities are unable to cooperate with the developers to allow the tracking of illegal activity[93].

Governance

The kind of organization in charge of updating and upgrading the network can take many forms:

- Decentralized governance: Fully not for profit open source, with changes agreed by most of the users (like Bitcoin and Ethereum),
- Centralized governance: For profit company with changes decided within a private company (Private blockchains)
- Hybrid models

However, there are some networks that claim to be decentralized which might be centralized - such as Binance Smart Chain (BSC) that Messari[94] analysts suspect it to be controlled by the centralized exchange Binance Chain. As the UK brank of the Binance corporation is not allowed to perform regulated activities in the UK[95], while the US branch faces probes for money laundering[96], BSC can suffer from association with Binance (despite the decentralized claims found in the website).

---

[91] http://blockchain.cs.ucl.ac.uk/blockchain-energy-consumption/ http://blockchain.cs.ucl.ac.uk/wp-content/uploads/2021/09/UCL_CBT_DPS_Q32021_updated-1.pdf

[92] https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html Pipeline Investigation Upends Idea That Bitcoin Is Untraceable.

[93] https://coinconfidential.com/is-monero-best-privacy-coin/

[94] https://www.financemagnates.com/cryptocurrency/news/is-the-binance-smart-chain-centralized-messari-researchers-raise-concerns/

[95] https://www.reuters.com/world/uk/financial-watchdog-orders-crypto-exchange-binance-stop-regulated-activities-uk-2021-06-27/

[96] https://www.bloomberg.com/news/articles/2021-05-13/binance-probed-by-u-s-as-money-laundering-tax-sleuths-bore-in





Identifying governance red flags requires deep analysis of the technology and the corporate structures set up by the developers.

The developer groups can dramatically change the structure of the network:

- From PoW to PoS;
- Strong cryptography method (to improve against quantum attacks);
- Transaction Per second;
- Payments to validators;
- Increase/decrease supply
- Etc;

Hence, the following points need to be monitored with extreme attention:

- Who proposes a change in the network's architecture ?
- Who develops the solution ?
- Who approves and releases the solution ?

For example, Ethereum can be upgraded by:

- Starting a Ethereum Improvement Proposal[97] (in theory anyone can propose, in practice there is a reputational pecking order - Vitali Buterin's proposal's attract higher priority).
- The proposal is reviewed by the EIP editors[98] for technical soundness and spelling mistakes (there has been some controversy surrounding editors[99])
- The proposal is approved by the EIP editors, the Ethereum Cat Herders[100] and the Ethereum magicians[101]

Besides the outsized impact of a small group of editors, developers can also be targeted by government regulations (like the US infrastructure bill who could impose fines to developers and validators[102], or extensions of the Chinese ban on crypto trading[103]).

---

[97] https://ethereum.org/en/eips/
[98] https://eips.ethereum.org/EIPS/eip-1 (includes updated list of Ethereum editors)
[99] https://steemkr.com/crypto-news/@pupinia/ethereum-code-editor-resigns-over-legal-concerns-for-ledger-amendment-proposal
[100] https://ethereumcatherders.com/
[101] https://ethereum-magicians.org/
[102] https://www.cohnreznick.com/insights/infrastructure-bill-expands-reporting-for-cryptocurrency-brokers
[103] https://www.coindesk.com/policy/2021/09/24/chinas-latest-crypto-ban-is-its-most-severe-insiders-say/

Programmable Governance resources: [104] [105] [106] [107]

Fourth Estate

Dr Keir Finlow-Bates introduced the concept of the **Fourth Estate**[108] as a set of organizations that can impact the distribution of information across all market participants; he uses a real life simile of the Press as organizations that can make a significant market impact.

Despite Twitter coming immediately to mind, his example is less obvious. The public ledger on Ethereum is public, but you would need to run a full Ethereum server to data mine it. Separate organizations have appeared that allow any person to do the data mining (like Etherscan.io[109]); however, while on the full Ethereum server you can access some of the soon to be 'orphan' chains, Etherscan only provides access to what it considers to be the valid chain - in effect providing instant credibility to that chain.

TODO - add list of other 4th estate

Validator Economics

Validators play a key part in a token ecosystem, not only because they maintain the ledger but also as:

- their incentives to either hold or exchange their tokens for fiat (or other tokens) can impact the price of the token versus fiat,
- They can become developers in order to influence the software upgrading and policy changes (usually to keep the status quo)

The following formula linking the token economy to the real life one comes from ([110]), and can be applied to other tokens (despite being devised for Ethereum)

***Economic Incentive Model** = Validator Rewards + Network Fees + Gain/(Loss) From Ethereum Price Changes – Costs To Be A Validator*

The formula can be re-written as:

$$EIM = (Validator\ Rewards + Network\ Fees + MEV) * Token\ Exchange - Costs\ to\ be\ a\ Validator$$

[104] https://thedailygwei.substack.com/p/valueless-governance-tokens-the-daily
[105] https://gov.uniswap.org/t/community-governance-process/7732
[106] https://messari.io/article/the-latent-power-of-governance-tokens
[107] https://medium.com/amentum/the-crypto-governance-manifesto-7c40df928b04
[108] https://www.youtube.com/watch?v=HjoyfgLZjoo
[109] https://etherscan.io/
[110] https://www.certik.io/blog/technology/validator-economic-incentive-model-ethereum





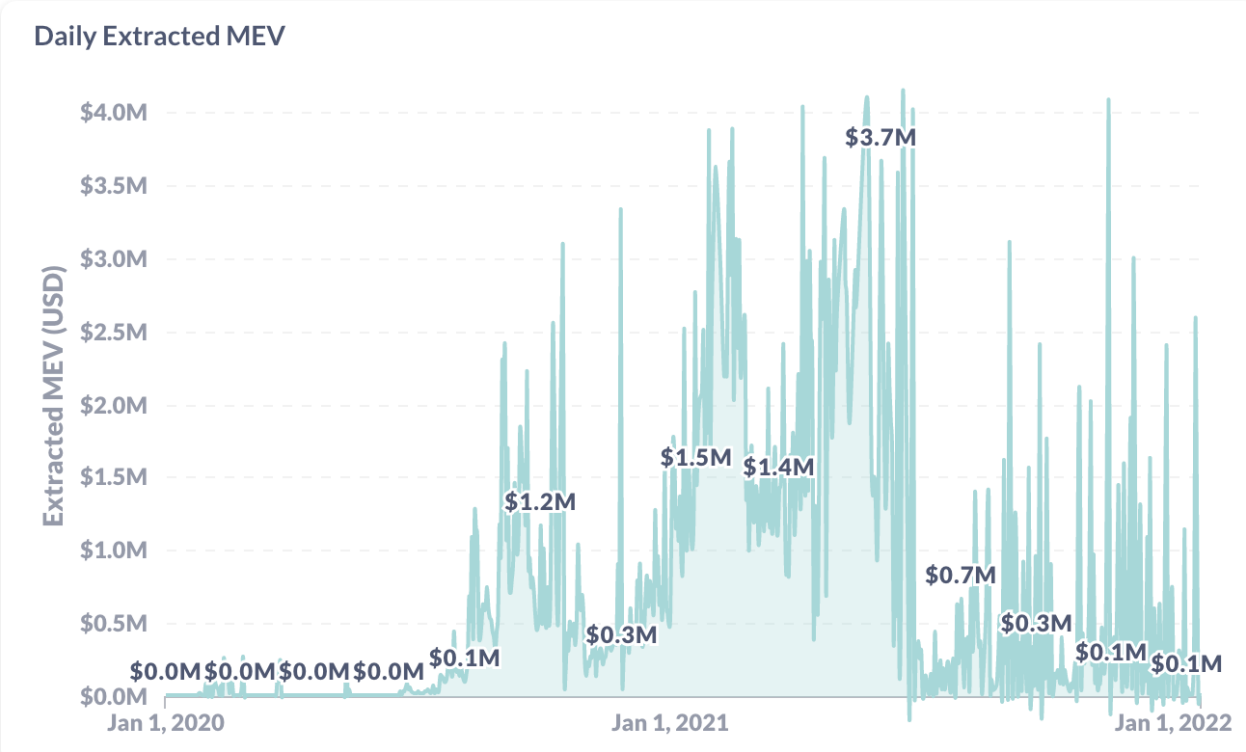
Validator rewards, *Network fees* and *Costs to be a Validator* are network dependent, they will be different for proof of stake or proof of work. *MEV* stands for Maximum Extractable Value which some Validators might perform for the token Ecosystems that allow it.
We could then assume that:

- Validators will exchange their rewards from tokens to fiat up to pay the *Cost to be a Validator.* (for example, computer depreciation, electric bills, salaries, rent, etc)
- Validators might hold the excess tokens and hope for token appreciation, or exchange into fiat/other tokens.

Maximum Extractable Value[111]

Indirect validators revenue: validators have access to valuable information which has been used to front-run other users - as the networks are not regulated this is not illegal, leaving the network governance to develop patches to either eliminate or reduce it. We highly recommend "*Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*"[112] as an introduction to the topic (although in the past it was used as a tutorial on **how** to do MEV).

[111] https://blog.chain.link/what-is-miner-extractable-value-mev/
[112] https://arxiv.org/abs/1904.05234



Project Flashbots[113] defines MEV as ...

> *"MEV (Maximal Extractable Value) is the total value that can be extracted permissionlessly (i.e. without any special rights) from the re-ordering, insertion or censorship of transactions within a block being produced. As miners currently have the ultimate say on transaction ordering and inclusion in Ethereum, they can be seen as the most powerful player in this game, hence the commonly used term Miner Extractable Value. Yet, MEV exists on any blockchain and layers where there is a party responsible for transaction ordering (eg. validators, rollup providers).*
>
> *Most of the MEV extracted on Ethereum today is captured by traders seizing opportunities where transaction ordering matters such as arbitrages and liquidations."*

... and has developed tools[114] to monitor MEV activity in the Ethereum network.

[113] https://github.com/flashbots/pm
[114] https://explore.flashbots.net/





Crypto valuation model

Once we have identified qualitatively the driving factors of crypto tokens, the next step is to incorporate them quantitatively in a valuation model.

Absolute Value

Most investors are familiar with the typical stock price target: '*XYZ company will reach $YYY by DATE)*'.

The first step is to identify available quantitative measures of the factors we identified above:

Supply	Stable, Inflationary, Deflationary. Inflationary tokens will include: • Coin Token Economics used by the Governance (Developers) to reward validators • Validators post-reward behaviour. Whale behaviour. (identify whales)
Demand	Utility: tokens purchased to be used in dApps: • exponential growth of applications will increase demand, • Growth of users per dApp • Growth of wallet users • Knowledge of transaction fees. Store of value: tokens purchased to hold. (possible manipulation in Social Media)
ESG	Governance: as supply can be modified by Developers, it is necessary to monitor carefully the governance and the Developer economic incentives. Quantitative measures are less well defined. Environmental: while at the moment there is no penalty against energy hungry networks, it is expected there will be. Social: We include Regulation in this area - networks which do not comply with the regulations of the largest economies could be penalized.





Fourth Estate	Identify 4th Estate actors.

The Supply part of a token is usually well known, leaving Demand as the main driver of price appreciation.

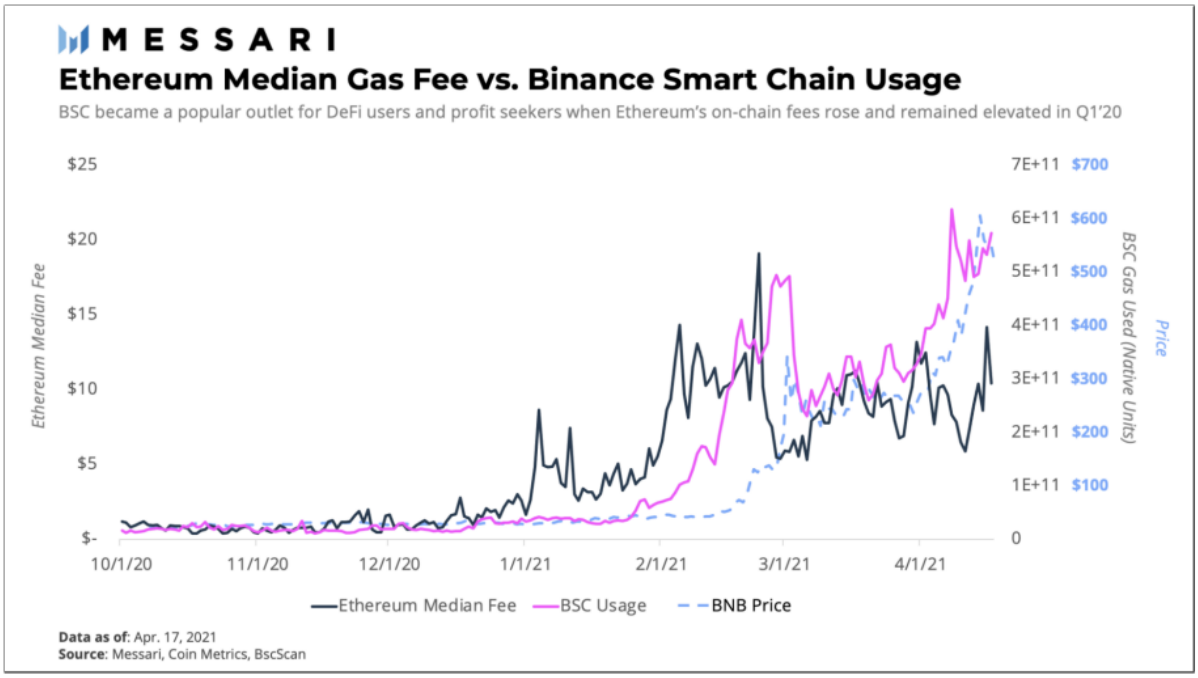
Price target = Price now + demand driven change

Relative Value

Investors are also familiar with the concept of relative value, in statements such as '*XYZ will outperform ABC in the following Time Period*'

The advantage of Relative Value models over absolute is the ability to remove factors that are difficult to measure or predict (e.g. Demand as a store of value driven by influencers)

Supply	Stable ?	Inflationary
Demand	No dApps ? Social Media hype ? Institutional Investors	dApp ecosystem growing / Scalable / low fee per transaction Unknown ?
ESG	Environmental: energy hungry Social: Anarchic Governance: Open Source	Environmental: energy hungry Social: Regulated in US Governance: Individual led
Fourth Estate	Open source	Government controlled



Gas dynamic is a driver of the store of value component. Of course, gas fees are paid in the L1 token as will all the derived dApp economy. Basing it into dollar terms becomes totally unmanageable for any ecosystem participant who is paid in fiat.

This is where system dynamics comes into play. Under certain growth assumptions, we can model the incentives, which leads us to a natural incentive system.

As described in our framework, relative value will constantly shift between blockchains.

In the near term based on capital flows and Total Value Locked. In the short term, attracting capital is the first step, alongside developer growth.

In the longer term, driven by governance economics.

In the bull case, these systems become very good at retaining capital.





Case Study: Ethereum Valuation

There are many introductory sources about Ethereum and tokens in general (see [115] [116]). What we will do is to deconstruct the network into the factors we have identified above.

We value ethereum like another financial asset decomposing it as having several components:

- **Staking** component which pays a yield (or dividend) to stakeholders.
- **Store of Value** component, which benefits stakeholders through capital growth.

Our model is driven by the store of value component which requires forecast. This is well understood and in a later section we will also forecast fees.

Some of the most important data for valuation is quantitative - such as total value locked in smart contracts. In particular we want to be able to measure 3 factors:

- Utility: measure the number of dapps on the ecosystem
- Cash Flows: reward economics
- Store of value: (1) stable, (2) speculative: use supply + demand + speculative; measure 'sticky hodlers', whales, -- liquidity depth measure (size of trade required to move the price)'

Dividend discount model

The bull case moving forward relates to two things.

(1) Scalability concerns.
(2) Ethereum competitors. If there are multiple interoperable blockchains and the effects of (1) are overcome by Ethereum 2.0, the competitors will not be able to gain momentum.

[115] Understanding Eth as an Investment (Dragonfly Research)
https://medium.com/dragonfly-research/a-guide-to-understanding-eth-as-an-investment-6f0f393db591

[116] Eth - the world's most valuable asset (Bizantine Capital)
https://apbakst.medium.com/eth-the-worlds-most-valuable-asset-802461f2b3e5

Factors

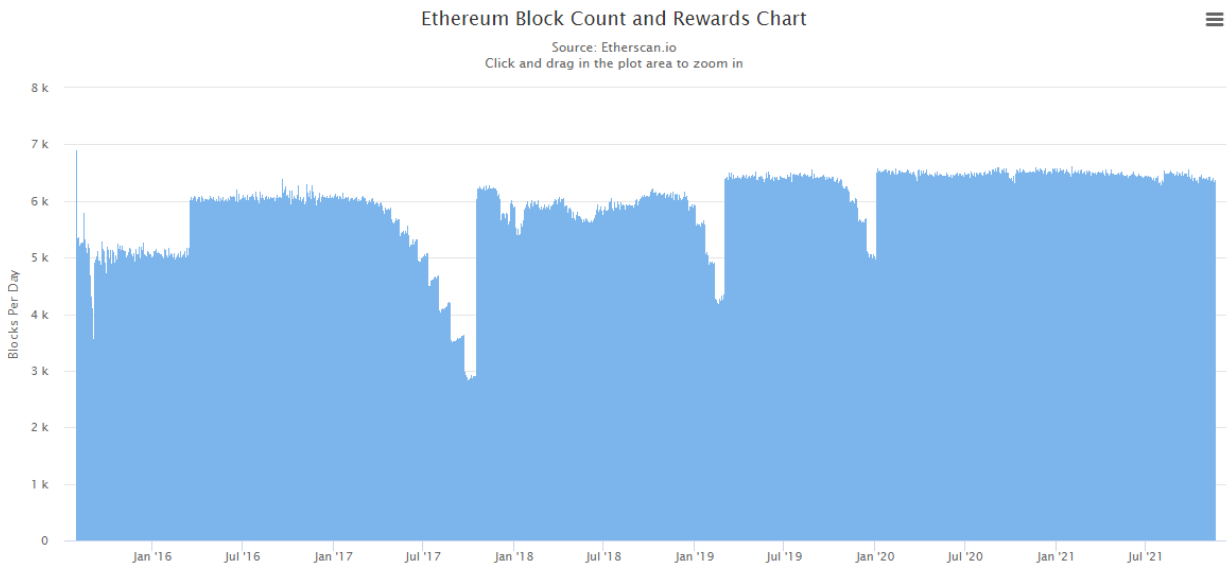
Supply

Unlike Bitcoin which famously has a fixed total supply of 21 million tokens, Ethereum creates new tokens as a reward for validators to incorporate new transactions into the decentralized ledger.Validators are rewarded for each block of transactions that is added to the ledger - however, the reward amount **can be modified** by the Ethereum community.

As a results, the daily supply of tokens is a function of the number of blocks minted times the reward per block[117].

- $Average\ Daily\ Blocks = 24\ hours * 60\ minutes * 60\ seconds / 13\ seconds\ per\ block = 6,646\ blocks.$

  The Average Daily Block number is constant at the moment: "*the average block time is between 12 to 14 seconds*" **enforced** with proof of work difficulty adjustments.



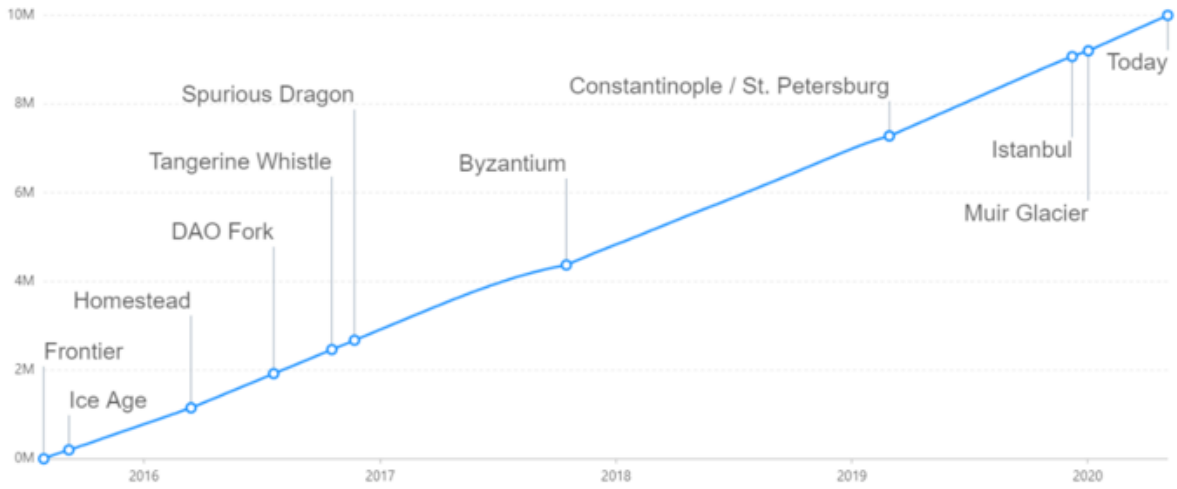
  - https://etherscan.io/chart/blocks

- Rewards per block are variable[118] and **can change** in the future:
  - At inception, it was 5 ETH per block,
  - Reduced to 3 ETH per block with the Byzantium hard fork,
  - Reduced to 2 ETH per block with the Constantinople hard fork,

[117] https://ethereum.org/en/developers/docs/blocks/
[118] https://coinguides.org/ethereum-supply/

- After the London Fork, ETH could become deflationary: ETH is burnt per block "*if the block reward is lower than the base fee burnt*"[119] - decreasing supply.

- The plots below shows the number of blocks mined over time (before the London Fork)



https://medium.com/mycrypto/the-history-of-ethereum-hard-forks-6a6dae76d56f

John Lubin (Ethereum co-founder) explains:

> *"So we're a fixed amount of gold on the planet. And the fixed supply of Bitcoin represents sound money to certain people. With $13 billion worth of Ether locked up in Ethereum 2.0 and $70 billion locked up in decentralized finance, we have enormous demand for the Ether token," Lubin said.*
>
> *"And now we're burning the Ether token with the introduction of the London hard fork," he added. London hard fork "doesn't mean that ETH immediately becomes a deflationary asset. For that to happen, ETH burned must be higher than ETH issued in block rewards." This is more likely after the move to proof-of-stake.*[120]

Given the above supply dynamics were trivial to compute pre-London Fork, but post London fork it is necessary to include estimates of burnt fees.

[119] https://finematics.com/ethereum-eip-1559-explained/

[120] https://www.bitcoininsider.org/article/122393/ethereum-becoming-ultrasound-money-consensys-founder-says

London Fork Miner Reward Economics

Above we described how the Ethereum network **directly** rewards the validators with newly created Ether tokens. However, validators get additional rewards[121] - pre London Fork they were:

Block Reward	2 ETH + Tx Fee + MEV

Where transaction fees [122] are a function of the market Ethereum Gas Price:

Term	Description
Gas	Unit for how much computation work is done.
Gas Price	How much you're willing to pay per gas for work (in gwei)
Tx Cost	Gas used * Gas Price
Gas Limit	Max gas you'll pay for a certain tx
Gas Block Limit	Max gas allowed in a block

Gas fees: Gas refers to the fee, or pricing value, required to successfully conduct a transaction or execute a contract on the Ethereum blockchain platform. The smallest unit of ether is a wei. Gas prices are measured in gwei (giga wei), also known as nanoether, since they represent a billionth of an ether i.e. 1e-9. The exact price of the gas is determined by supply and demand between the network's miners.

[121] https://2miners.com/blog/ethereum-london-hardfork-what-does-eip-1559-change/

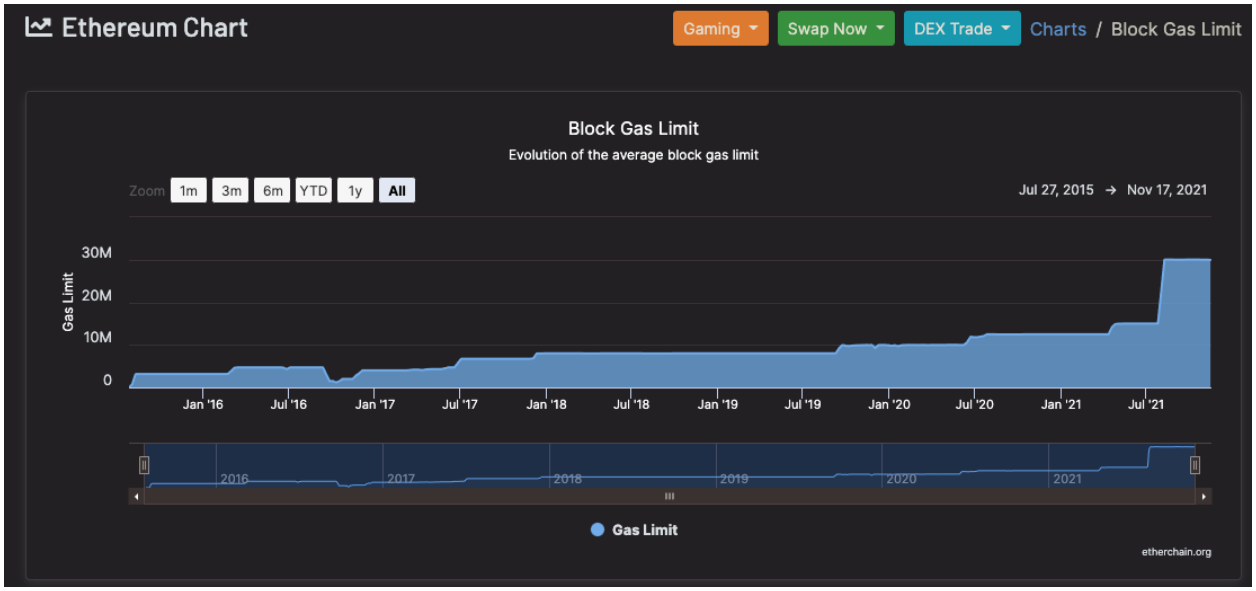
[122] https://medium.com/@eric.conner/understanding-ethereum-gas-blocks-and-the-fee-market-d5e268bf0a0e

Maximal Extractable Value (or Miners EV - MEV) is beyond the scope of this paper, but we encourage you to read ([123]).

For a Validator (Miner using the term above, but expected to change when Proof of Stake is introduced) the Block Reward would be:

$$Block\ Reward\ =\ 2\ ETH\ +\ Gas\ Block\ Limit\ \times\ Gas\ Price\ +\ Maximal\ Extractable\ Value$$

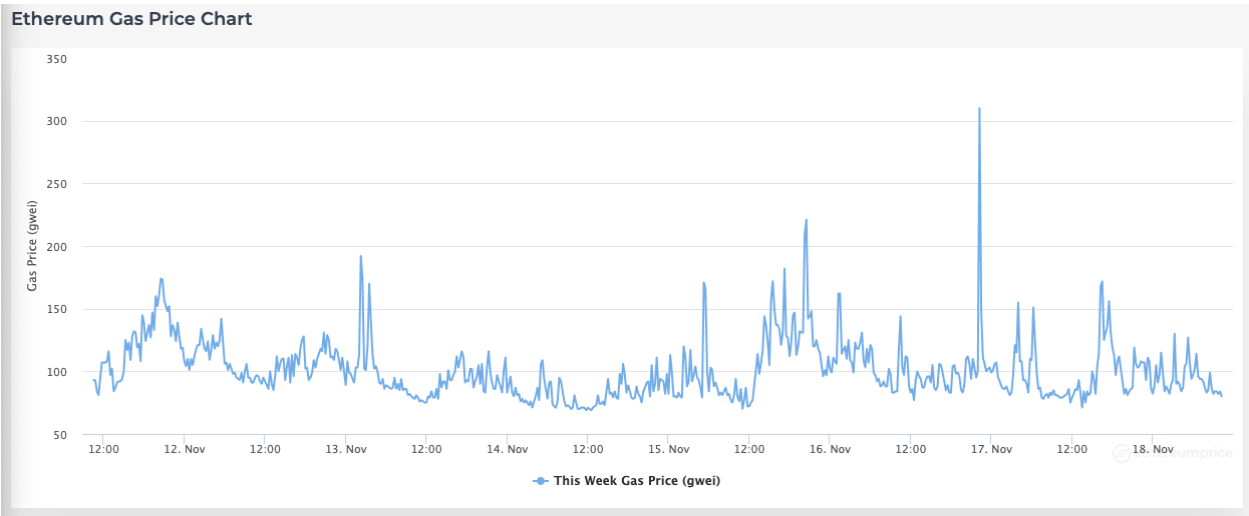
The Gas Block Limit is defined by the validators and can change over time (but competition around validators should in theory limit their ability to game it - on the other hand, it is a factor to consider in other networks):



https://www.etherchain.org/charts/blockGasLimit

But the Gas Price is a function of supply and demand of transactions particularly of computationally intensive smart contracts.

[123] Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges https://arxiv.org/abs/1904.05234



https://ethereumprice.org/gas/

(read [124] for a detailed list of events that have changed the Gas Price)

After the London fork, the reward formula changes for Validators change to

$$Block\ Reward\ =\ 2\ ETH\ +\ Inclusion\ fee\ +\ Maximal\ Extractable\ Value$$

Where the optional Inclusion fee is a 'tip' from users who want priority. The users will still pay the Transaction fee ($Gas\ Block\ Limit\ \times\ Gas\ Price$) which will be burned - leading to a deflationary dynamic when $Transaction\ fee\ >\ 2\ ETH$:

$$\text{Ether reduction } \Delta ETH_{circulating\ supply}\ =\ (2\ ETH\ -\ Transaction\ fee)\ .$$

Ethereum 2.0 Merge

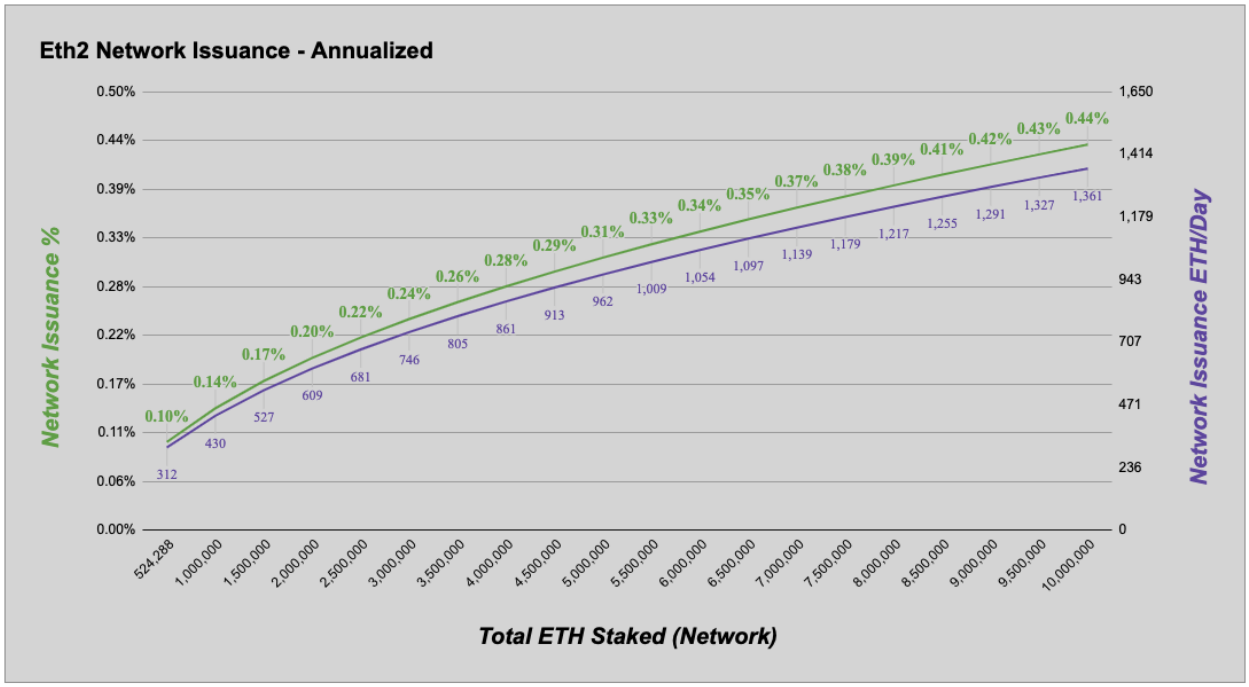
In Q2 2022[125] Ethereum is expected to move validation from Proof of Work to Proof of Stake. Rewards in POS are expected to be "*5-10x lower than rewards from proof-of-work*"[126], with

$$\Delta ETH_{circulating\ supply}\ =\ \frac{2\ ETH}{(5\ to\ 10)}\ -\ Transaction\ fee$$

Leading to further deflationary forces when the Transaction fee per block increase.

[124] https://blog.mycrypto.com/the-history-of-ethereums-block-size-block-gas-limit/
[125] https://ethereum.org/en/eth2/merge/
[126] https://cryptonews.net/en/news/ethereum/2431549/

The 5-10x is only an estimate - there is an open source calculator used to estimate Annual Network issuance[127]



(e.g. at ETH10mn staked, the network could issue 1,361ETH/Day)

Reward Economics (what do the new coin holders do with the supply) - hold or sell ?

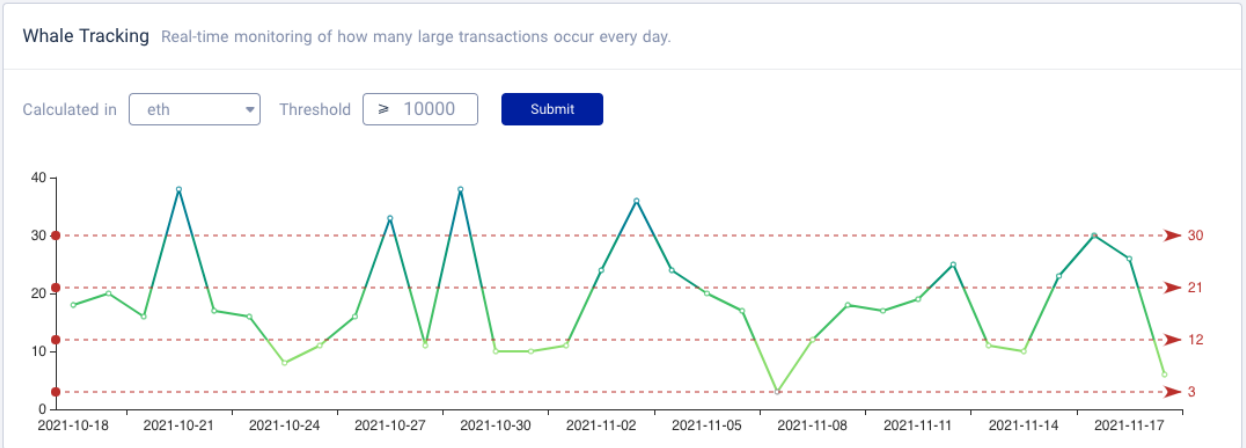
> *The purpose of inflation in any layer-one cryptocurrency is to pay miners for security*
>
> *Testament to the level of excitement around Ethereum in Q2 2021 was the vast amount of capital being moved around on-chain, and institutions starting to see the huge potential in the programmable money blockchain as it births vast new subsectors of cryptoassets in DeFi and NFTs.*
>
> *While Ethereum's ever increasing usage is an excellent sign for the long-term prospects of the network, in the near term the growing pains that we have seen throughout its*

[127] eth2 Calculator (Main)
https://docs.google.com/spreadsheets/d/15tmPOvOgi3wKxJw7KQJKoUe-uonbYR6HF7u83LR5Mj4/edit#gid=1494215209

lifespan to date: notably high 'gas' or transaction fees for carrying out on-chain work, have continued to proliferate.

Whales

Accounts with large holdings of Ethereum can be tracked using the blockchain explorers (e.g. [128])



Transaction — Total 594 — First < 1 2 3 4 5 > Last — Go to Page

Hash	Height	From	To	Amount	Time
0x19c4b9...	13638574	0x28c6c0...	0x4976a4...	25,147.00685496 ETH	4 hours ago
0x37e6b4...	13638250	0x28c6c0...	0x21a31e...	25,230.71508551 ETH	5 hours ago
0x04a9b4...	13637422	0x28c6c0...	0x56eddb...	25,156.23208197 ETH	8 hours ago

Demand

Fat Protocol Theory

For every $1 of value created by Ethereum's application, x% of that trickles down to ETH.

[128] https://eth.tokenview.com/en/largetxs

Further, this would cement the idea that token economics and adoption is the winning formula for a successful base layer. If teams build strong incentives on the base layer to create working applications and allow those applications to drip value into the base blockchain by funneling in more users, everyone wins.

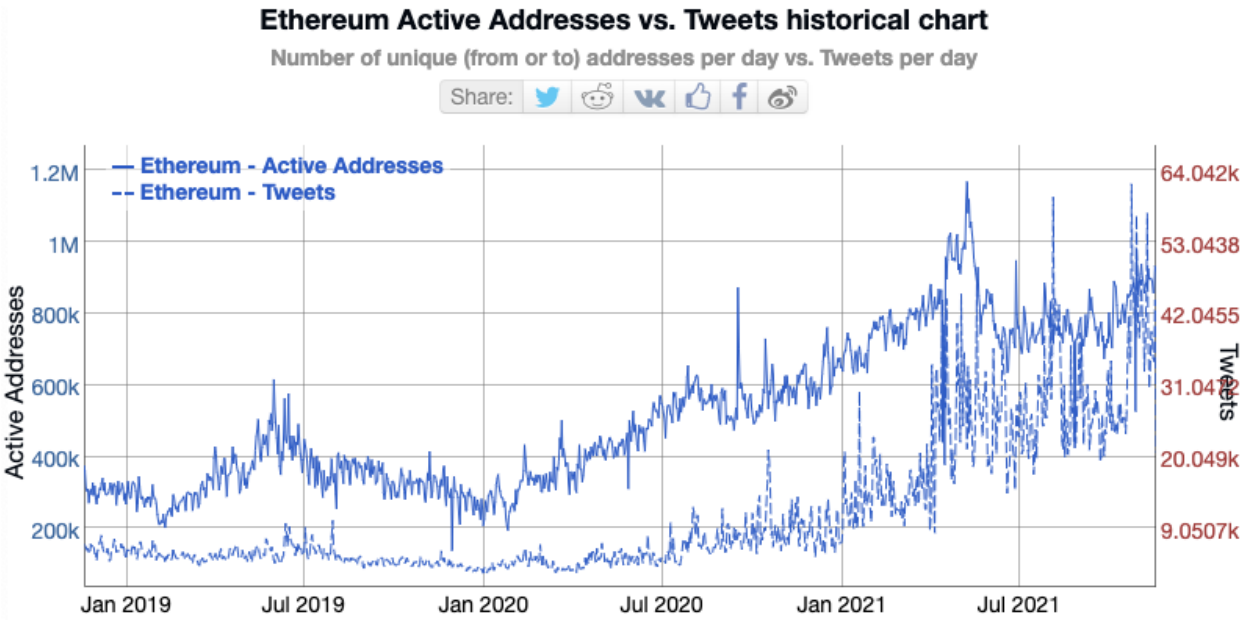
Retail Investors

Retail investors who purchase ETH can be proxied by looking at Centralized Exchange Flows and wallet growth with a lower than median ETH amount.

The purchases can be allocated in two different ways

- As store of value,
- As medium of exchange and to pay transaction fees.

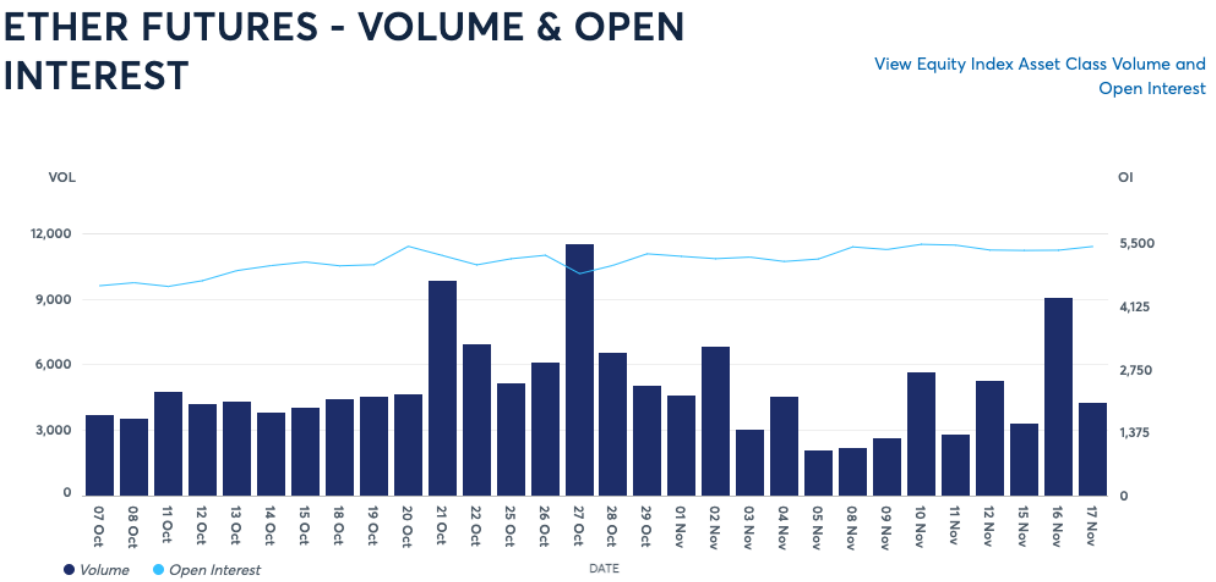
For example, the number of active addresses[129] has tripled since Jan 2019 (highly correlated with the number of tweets about Ether):



[129] https://bitinfocharts.com/comparison/ethereum-activeaddresses.html#3y

Institutional Investors (regulated)

Regulated institutional investors need to invest in regulated markets such as the CME ether futures[130]:



At the moment there is speculation[131] an Ether futures ETF will be launched following the steps of the ProShares Bitcoin ETF[132].

In Q2 Andreessen Horowitz (a16z) launched two crypto funds, first a $515m fund on 30 April 2021, followed by one quadruple the size on 24 June 2021 at $2.2bn. Much of this investment is expected to flow into Ethereum-based products and services.

In the near future is also possible public companies (like Microstrategy[133] or Tesla) start allocating capital to ETH - once they do so, their assets might have to be disclosed publicly (e.g. [134]).

---

[130] https://www.cmegroup.com/markets/cryptocurrencies/ether/ether.volume.html

[131] https://www.morningstar.com/news/marketwatch/20211024182/an-ether-futures-etf-is-next-likely-step-after-proshares-watershed-bitcoin-moment-a-former-sec-official-explains

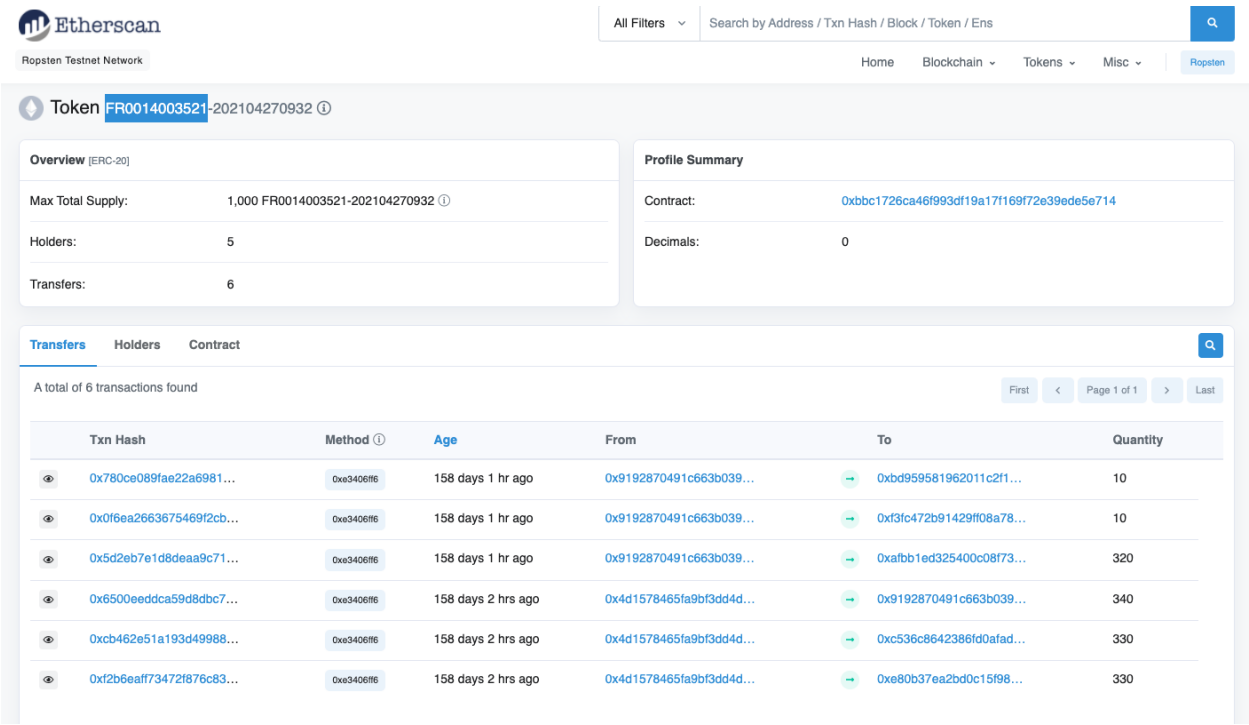
[132] https://finance.yahoo.com/quote/BITO/

[133] https://cryptonews.com/news/bitcoin-mega-bull-microstrategy-ceo-gives-hope-to-ethereum-a-10711.htm

[134] https://www.microstrategy.com/en/investor-relations/press/microstrategy-announces-first-quarter-2021-financial-results

EIB Bond Issued on Ethereum[135].

There are not many details, but the bond (Isin code FR0014003521) can be found on the test Ethereum network (Ropesen) using etherscan[136]:



Institutional Investors (unregulated)

The rapid price appreciation of tokens has created a large set of non regulated corporations (as opposed to individuals) who hold cryptocurrencies. Some of them have already been identified as Whales, but their behaviour will differ from HODL investors as they could be more proactive - exchanging their ETH into other currencies or viceversa.

CBDC

Ethereum has been used in Central Banks (U.A.E., Bank of Thailand) cross transfer prototypes (see [137] page 41) :

---

135 https://www.eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain

136 https://ropsten.etherscan.io/token/0xbbc1726ca46f993df19a17f169f72e39ede5e714

137 https://www.bis.org/publ/othp40.pdf Inthanon-LionRock to mBridge

"This tokenisation was done using the Universal Token standard developed by ConsenSys. Universal Token is a smart contract standard that extends the ERC-20 and ERC-1400 smart contract standards, some of the most popular token standards on the Ethereum blockchain. ERC-20 defines a set of functions that enable smart contracts to provide token-like functionality.46 ERC-1400 extends the functionality of the ERC-20 contract and enables functions for regulatory compliance, fractional ownership, fungibility, and issuer forced transfers."

Decentralized Applications

Decentralized applications (dApps) like Decentralized Finance (DeFI) have grown exponentially since last year.

In ([138]) we can see the top 5 Ethereum DeFI applications at the moment (using Total Value Locked TVL):

				CAP	ATVL	TVL	CAP/TVL
1	Curve	ETH • Polygon	BUY	$6.51B +1.01%	$14.75B +2.82%	$16.77B -0.13%	0.39
2	Oasis App	ETH	BUY	$2.91B +6.6%	$11.53B +2.5%	$15.09B -1.77%	0.19
3	WBTC	ETH	BUY	$14.36B -2.3%	$11.52B +5.28%	$14.36B -1.56%	1
4	Compound	ETH	BUY	$3.04B -5.03%	$9.28B +4.29%	$11.31B +0.03%	0.27
5	Aave	ETH • Polygon	BUY	$4.37B -2%	$10.09B +3.38%	$11.25B -1.22%	0.39

And the 9 fold growth from 16bn TVL one year ago to 142bn now.

[138] https://dappradar.com/defi/protocol/ethereum



The growth is important as every transaction in one the the DeFI requires a fee (the transaction fee described above) which needs to be paid in ETH.

Furthermore, dApps validate the **intrinsic value** of ETH, as it becomes **useful** and dApp developers become

Network Effects / Development communities

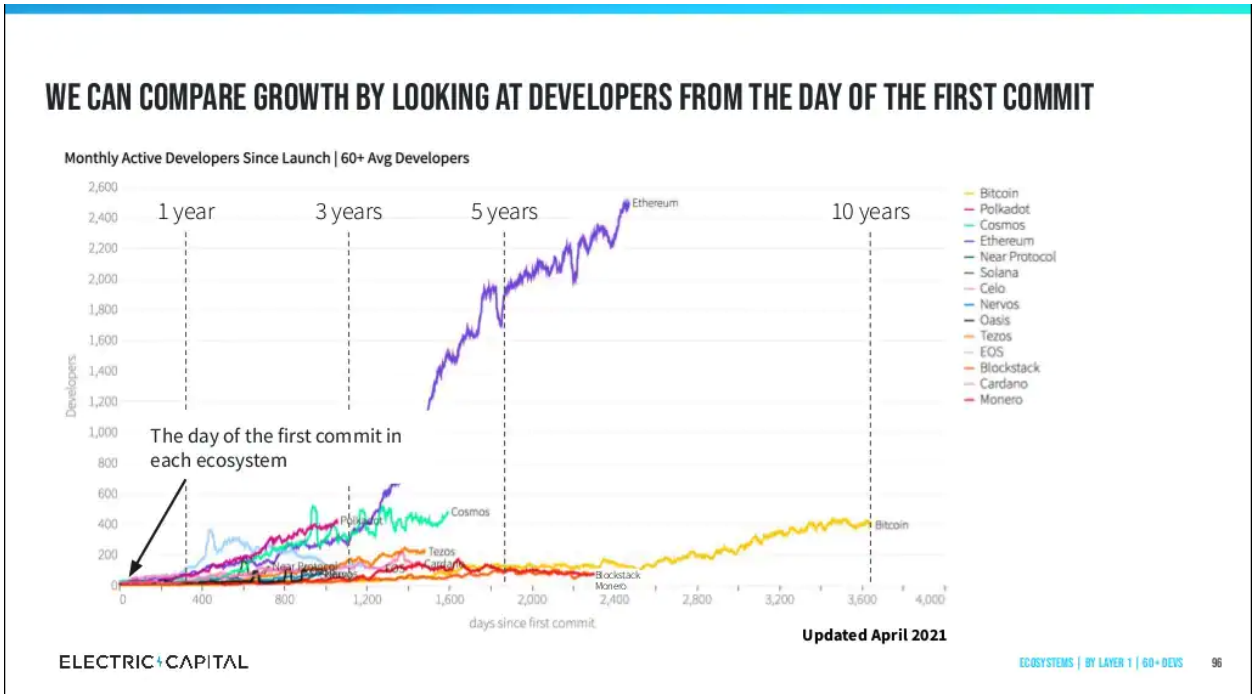
> *"Being defined by DeFi is better than being defined by nothing. But it needs to go further."* - Vitalik

Ethereum Has Stronger Network Effects Than Bitcoin.

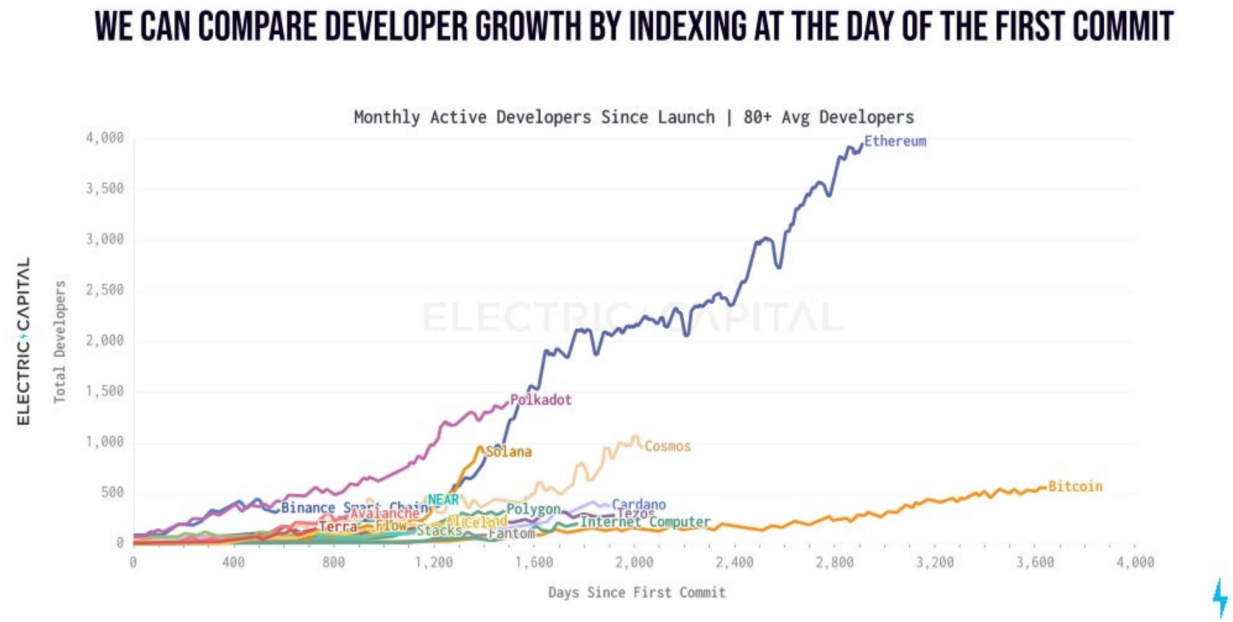
> *"Ethereum to me has a much higher utility [than Bitcoin] through smart contracts...suddenly something shows up and your Walkman looks like an abacus."*
>
> Todd Morley, Guggenheim co-founder, speaking on Bloomberg TV

Smart Contract developments such as ERC20 begat instruments like non Fungible Tokens (NFT's) which in turn begat NFT minting and trading dApps such as Opensea.

Profitability of dApps attracts more software developers[139] [140] [141]- see the growth from April 21 …



… to December 2021…



[139] https://electric-capital.github.io/ for a list if git repositories per ecosystem
[140] https://medium.com/electric-capital/electric-capital-developer-report-2020-9417165c6444
[141] https://medium.com/electric-capital/electric-capital-developer-report-2021-f37874efea6d





... which encourages them to keep the status quo (after learning how to develop and audit dApps in one ecosystem, incentives to port the code to another one should be high).

Additionally, part of Ethereum's attractiveness to institutional finance professionals and beyond is that it is inherently multi-asset. With that in mind, it is also worth noting that Wrapped Bitcoin — the ERC-20 tokenised version of Bitcoin traded on top of Ethereum — has risen over 2,000% YOY and now represents approximately 1% of Bitcoin's total supply. Make of that what you will.

Layer 2 Protocols

In ([142]), Keir Finlow-Bates estimates that in November 2021 the cost of minting 10,000 NFTs on Ethereum is one million dollars.
Despite urban legends that Ethereum can only handle about 20 transactions per second (tps - 1.7million per day) compared to VISA's 24,000 tps, there is no fixed limit to it (as shown previously - the gas limit per block can be increased). The basis for the legend might come from data such as[143]:

[142] https://www.linkedin.com/pulse/how-calculate-ethereum-gas-prices-keir-finlow-bates/
[143] https://decrypt.co/35962/ethereum-approaches-technical-limits-as-transactions-soar

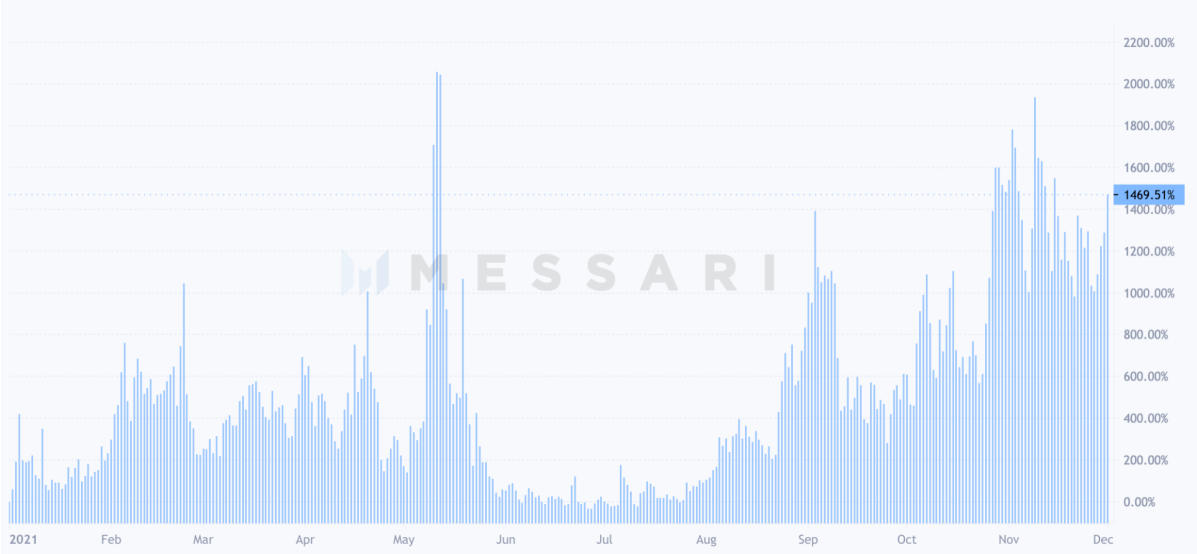


Ethereum daily transactions chart. Source: Etherscan

The high transaction fee is a method to solve the inexistent scalability of Ethereum (called the trilemma[144] as scalability in Ethereum was sacrificed to obtain security and decentralization). This pricing reduces the number of possible dApps and dApps users.

Median Transaction Fees

[144] https://www.cryptocompare.com/coins/guides/what-is-the-blockchain-trilemma/

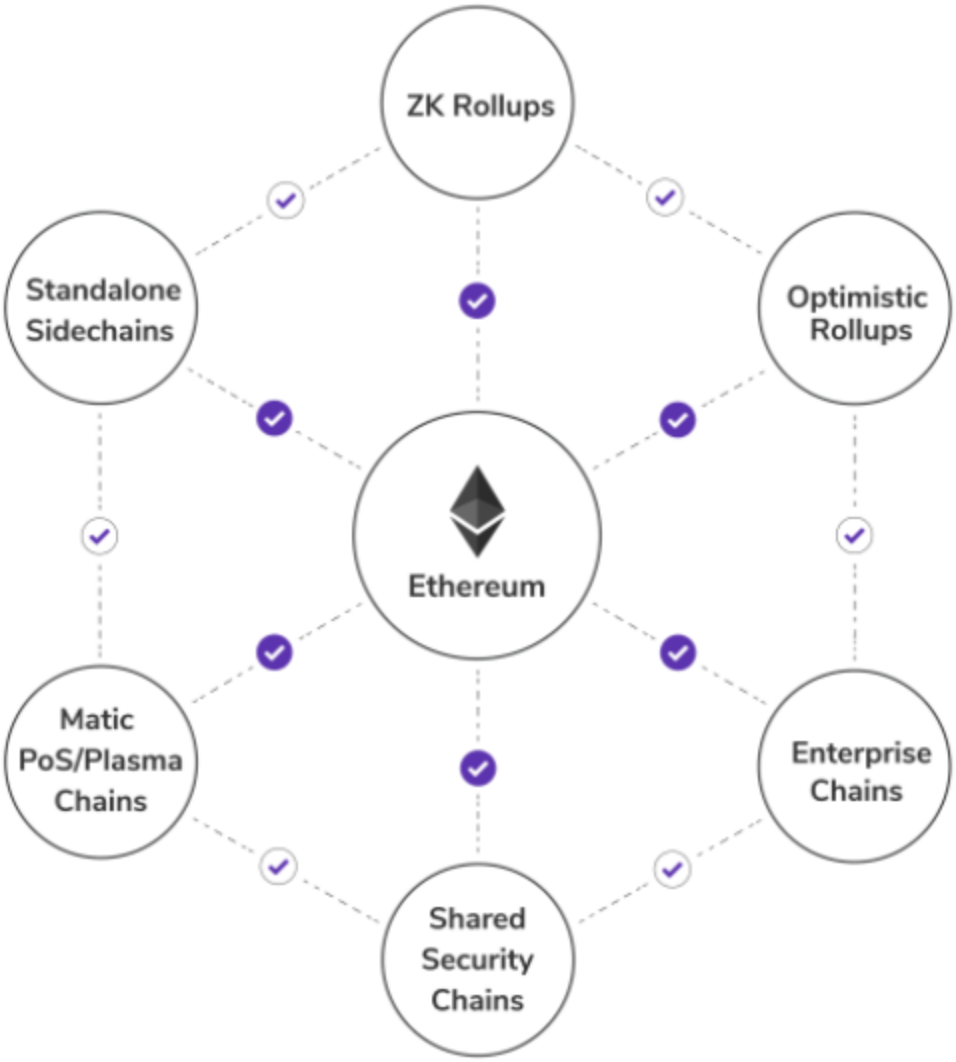


There are two approaches to solve this problem:

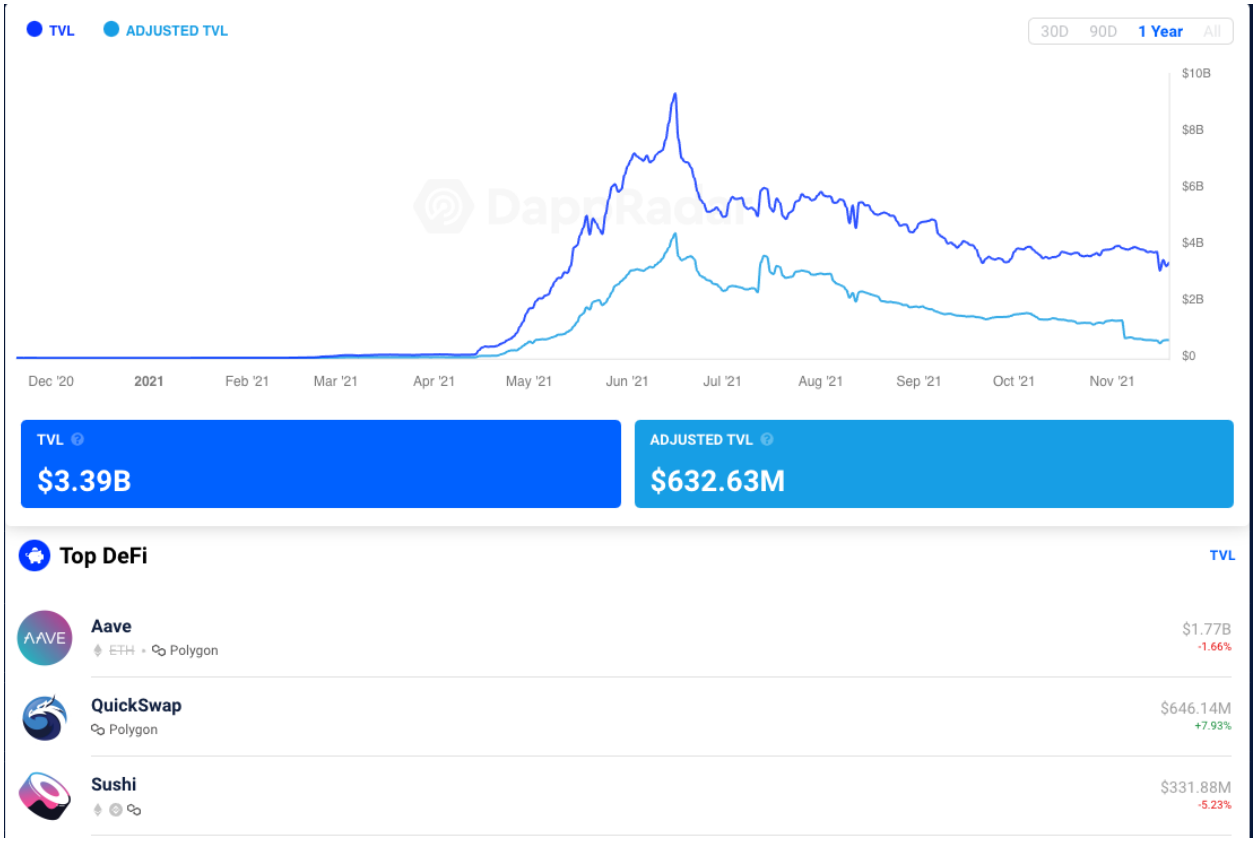
- The fabled Ethereum 2.0 upgrade (estimated to be merged in Q2 2022),
- Layer 2 networks[145] such as Polygon[146] which are networks that use the Ethereum network as a backbone (details are beyond the scope of this paper) and as such,

[145] https://www.finextra.com/blogposting/21237/top-ethereum-layer-2-networks
[146] https://polygon.technology/

require ETH to run.



Ethereum 2.0 might very well put the layer 2 networks out of business, but while it happens, we can monitor their growth and decline[147]:



Validator Economics

At the moment, validators are much better compensated by the 'validator reward' (2 ethereum by block - total capped daily) than by Network fees ([148] [149]).

Yield

Proof of stake network introduce the concept of **staking[150] yield** which is an (almost) token risk-free return for tokens that are staked in a pool. There are other possible sources of yields (see DeFI) but they include either credit or FX risk.

[147] https://dappradar.com/defi/protocol/polygon
[148] https://consensys.net/blog/codefi/rewards-and-penalties-on-ethereum-20-phase-0/
[149] https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-economics/

[150] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

The staking yield can become an incentive to carry investors, specially while the interest in banks is below it (at the moment of writing the yield is 5.2%[151] [152] per year).
The yield is determined using the following formula[153]:

$$yield = e^{\left(\frac{31556926}{384} \times \frac{64}{31622 \times \sqrt{ETHstaked}}\right)} - 1$$

(see [154] for the meaning of the numbers)

As the number of ETH staked grows, the yield decreases.

ESG

Environmental

Proof of work is condemned[155] by researchers for its energy consumption characteristics. As Regulators and governments penalize companies and investors in carbon producing industries, proof of work tokens need to decrease in value to reduce the complexity of the proof (as a rule of thumb, higher price of a token attracts more Miners - to keep the number of reward tokens constant the work complexity increases, which requires larger energy consumption).

Ethereum merge[156] with the beacon chain proof of stake should future-proof and shield ETH from government ESG regulations.

Social

Tokens used for money laundering and terrorism activities have given crypto a dubious reputation. Paradoxically, because both Bitcoin and Ethereum are both pseudonimous (not fully anonymous) and have public ledgers, it is easier [157]to track the transactions of malicious agents.

---

[151] https://ethereumprice.org/eth-2-calculator/
[152] https://launchpad.ethereum.org/en/
[153] https://twitter.com/VitalikButerin/status/1326444925957754880
[154] 31556926 = seconds per year, 384 = seconds per epoch, 31556926 / 384 = epochs per year, 64 = BASE_REWARD_FACTOR, 31622 = sqrt(gwei per ETH).
[155] https://www.cityam.com/will-esg-turn-bitcoin-into-a-digital-stranded-asset-or-monetary-myspace-part-i/
[156] https://ethereum.org/en/eth2/merge/
[157] https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html

The Ethereum community has shown resolve to reverse fraudulent transactions (e.g. [158]) on the blockchain (which leads to the next topic - Governance).

Governance

The Ethereum community[159] apparently spouses a Decentralized governance mode[160]:

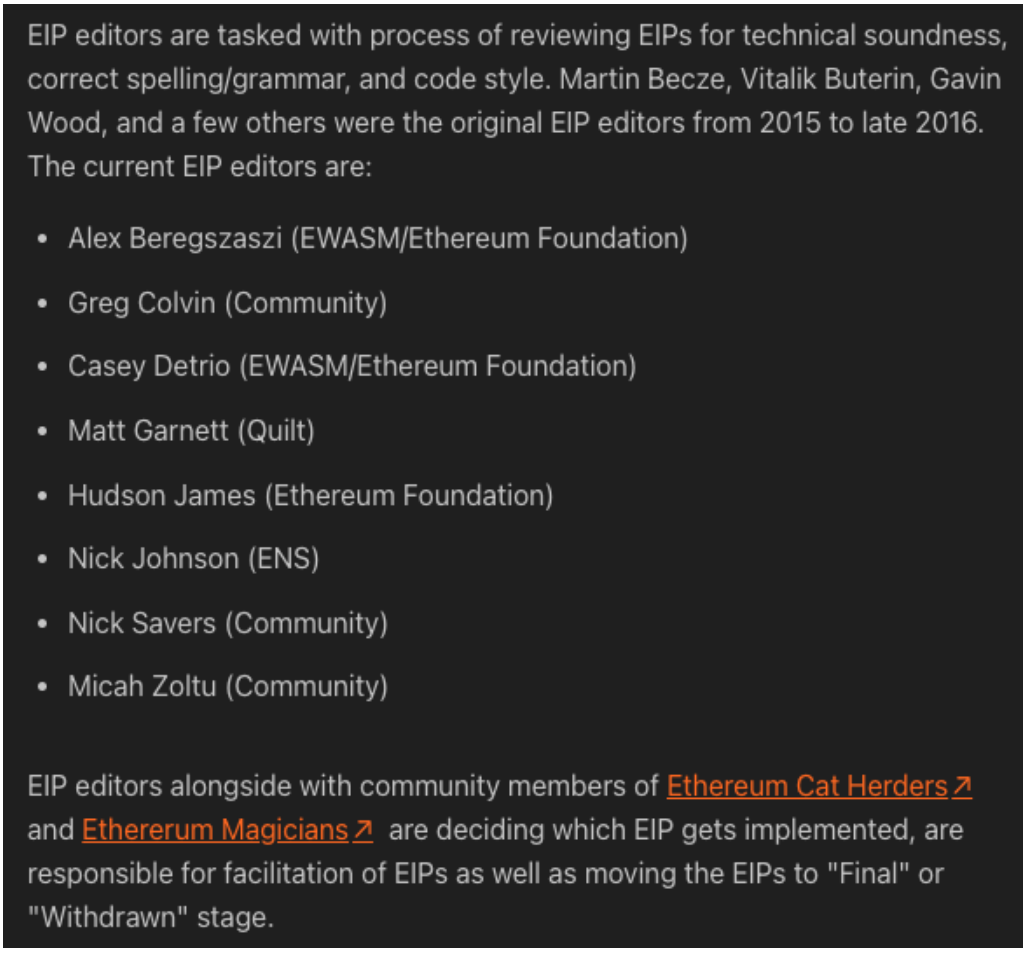
> The opposite approach, off-chain governance, is where any protocol change decisions happen through an informal process of social discussion, which, if approved, would be implemented in code.
>
> **Ethereum governance happens off-chain** with a wide variety of stakeholders involved in the process.

According to ([161]) "*One important process used in Ethereum governance is the proposal of Ethereum Improvement Proposals (EIPs). EIPs are standards specifying potential new features or processes for Ethereum*." (e.g., EIP 1559[162] which changed the reward structure for Validators).

In practice, the EIP editors[163] hold outsized influence (specially Vitalik Buterin):

[158] https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/
[159] https://ethereum.org/fa/community/
[160] https://ethereum.org/fa/governance/
[161] https://ethereum.org/fa/governance/#what-is-an-eip
[162] https://eips.ethereum.org/EIPS/eip-1559
[163] https://ethereum.org/fa/eips/





Despite their claim that 'anyone' can be a proposer, notice that the main author of EIR 1559 is Vitalik Buterin (and no, it is not alphabetical order, as the last author is named as Abdelhamid Baktha).
It is possible the founders step back just as Satoshi Nakamoto did with Bitcoin, but that might make future changes dominated by Validators whose priorities will be to keep the status quo instead of innovation and further ESG improvements.

Fourth Estate

Etherscan has become the accepted[164] publisher of Ethereum data:

164

https://medium.com/coinmonks/whats-the-best-ethereum-block-explorer-10-alternatives-to-etherscan-8eb5f2be263d





> The original and overall best block explorer for Ethereum. You can check pretty much anything, diving deep into mined blocks, transactions and addresses. It's got a load of other cool tools like checkers for gas, nodes and DEXs, along with some interesting charts & stats.

However, anyone can run a validator/miner node and examine the transactions before they are incorporated into the blockchain - in fact, this is crucial for Validators who engage in Maximal Extractable Value techniques.

Supply and market cap stats:	https://etherscan.io/stat/supply
Block count and rewards chart:	https://etherscan.io/chart/blocks
Supply growth chart:	https://etherscan.io/chart/ethersupplygrowth
Average block time chart:	https://etherscan.io/chart/blocktime

The power of the 4th estate lies in its ability to independently judge which one is the correct ledger. Having decentralized ledgers means that at any time there might be different possibilities of which transactions have been done - the 4th estate becomes the arbiter of the right one, and **source of the indicators** we have shown to you above.

Sophisticated agents will set up their own[165] ethereum nodes as that will allow them to review transactions before they are published (and the most sophisticated one will run MEV strategies).

Ethereum Technical Outlook

In the sections above we have discussed multiple time changes on the Ethereum network and their possible price.

To summarize, at the moment Ethereum:

---

165 https://medium.com/@JustinMLeroux/running-ethereum-full-nodes-a-guide-for-the-barely-motivated-a8a13e7a0d31



- Is a proof of work network which increases the complexity of proof required for Validator rewards as more Validators compete for it. As a result, more energy is required when the price of ETH increases.
- Offers Turing complete smart contracts (which allow the development of sophisticated dApps).
- Is highly secure and decentralized, but not scalable - which leads to high transaction fees as means to limit the number of transactions per second.
- Has a lightly inflationary/even deflationary token supply after implementation of EIP1559.
- Is theoretically open source, but in practice changes are dominated by the founder (Vitalik Buterin)
- Layer 2 networks (not sanctioned by Ethereum) have appeared to solve the scalability issue.

Planned changes (Ethereum 2.0):

- Proof of stake will replace proof of work, hopefully reducing energy consumption.
- Risk free yield is introduced in ETH space (for reliable validators). Penalties for malicious/unreliable validators are introduced.
- Sharding[166] is introduced as a method to solve scalability issues and reduce transaction fees.

Proof of Stake Explained

‘ Consensus mechanisms (also known as consensus protocols or consensus algorithms) allow distributed systems (networks of computers) to work together and stay secure. ‘ - Ethereum Foundation

Consensus participants allocate scarce economic resources, in exchange for a reward. And the byproduct of that is that it builds and secures the system.

In proof of work, that is hardware and energy and in proof of stake it's actually the native in-protocol token itself.

There different ‘flavours’ of proof of stake available[167]:

[166] https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/sharding/
[167] https://www.algorand.com/technology/pure-proof-of-stake





- **Delegated Proof of Stake (DPos)**: a fixed number of elected entities, delegates, are selected to create blocks in a round-robin order, allowing for scalable transactions per second. It is vulnerable to denial of service attacks on the limited amount of entities[168].
- **Bonded Proof of Stake (BPoS)**: any number of users set aside part of their stake (i.e., bond) in order to influence block generation. They lock up part of their stake for a certain amount of time (like a security deposit), and in return they get a chance proportional to that stake to select the next block (e.g. Solana)
- **Pure Proof of Stake (PPoS)**: users are *randomly* and secretly selected to propose blocks and vote on block proposals. The likelihood that a user will be chosen, and the weight of its proposals and votes, are directly proportional to its stake.

Ethereum is a BPoS, which implies that the users with the largest stake have access to the transaction information before other users - which allows them to engage in Maximum Extractable Value (MEV)[169].

So the locking up and allocation of ether to this protocol allows a user to participate in the protocol as a byproduct, secure protocol by verifying size and order of transactions.

The building blocks of the system, the native token, ETH can be valued as a financial asset.

> *"Instead of using computational resources to verify the next block, Ethereum 2.0 will rely on ETH holders (validators) to vote on the next block, making the security model based on game theory and economics. Ethereum 2.0 will also split the network into 64 shards that will parallelize the network and allow for it to scale in the future."*

The Beacon chain is a highly sophisticated proof of stake consensus mechanism.

Governance and staking. The risk of so many interoperable blockchains that demand for any one token has no scarcity value. We argue that this is not the case. We quantify the network effects.

PoS Smart Contract Platforms

Smart contract, proof of stake ecosystems create genuine value through their tokens that give access to participate in an ecosystem.

[168] https://decrypt.co/81375/solana-blames-denial-of-service-attack-for-last-weeks-downtime
[169] https://explore.flashbots.net/





Pros	Cons
Staking makes it easier for you to run a node. It doesn't require huge investments in hardware or energy, and if you don't have enough ETH to stake, you can join staking pools.	Proof-of-stake is still in its infancy, and less battle-tested, compared to proof-of-work
Staking is more decentralized. It allows for increased participation, and more nodes doesn't mean increased % returns, like with mining.	
Staking allows for secure sharding. Shard chains allow Ethereum to create multiple blocks at the same time, increasing transaction throughput. Sharding the network in a proof-of-work system would simply lower the power needed to compromise a portion of the network.	

Ecosystem Revenue

Metric	Q3 '20	Q3 '21	Y/Y
Network Revenue (Billions)	$321,213,004.34	$1,961,136,715.74	511%
Value Settled	$107,751,444,461	$536,488,443,460	398%
ETH Staked	0	7,559,965.00	-
ETH Issuance Rate (Quarterly)	1.11%	0.79%	-29%
Value of ETH Burned	0	$1,339,710,211.70	-
Daily Active Addresses	368,467.00	457,402.00	24.1%
DeFi TVL	9.23	$123.90	1242%
Dex Volume (Billions)	$48.27	$189.16	292%
Stablecoins Issued (Billions)	$13,622,000,000.0 0	68,770,000,000	405%
Money Market Borrow Volume (Billions)	$1,279,000,000.00	$16,090,000,000.00	1158%
BTC on Ethereum	123,500	288,234	133%
OpenSea Sales	$4,760,692.00	$6,757,656,242.00	141847%
L2 TVL	$8,410,232.18	$2,513,450,206.10	29786%
Hash Power (GH/S)	250,888.48	705,663.72	181%

170

Discussion: Ecosystem revenue is predefined by governance - the developers decide both the amount of ether to be distributed among validators and are able to modify the network fees[171] [172] at will -- e.g., Algorand can reduce the fees if their price exceeds values readily accepted by users.

[170] https://www.benzinga.com/markets/cryptocurrency/21/10/23740517/heres-what-ethereums-q3-2021-report-would-look-like-network-revenue-up-511-to-1-96b
[171] https://ycharts.com/indicators/ethereum_network_transaction_fees_per_day
[172] https://ycharts.com/indicators/ethereum_block_rewards_per_day





References

Online

"HMRC internal manual Cryptoassets Manual"[173]

Introductory books

"Blockchain Investor Manual", by Kosrow Dehnad, Joe Duncan[174].

"Move Over Brokers, Here Comes the BlockChain", by Dr. Keir Finlow-Bates[175]

[173] https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10350
[174] ISBN-13 979-8637258871
[175] ISBN-10 1688289976