Monetary Wars

The Role of Money in the Digital Asset Era

Abstraction Capital

22 March 2022

Abstract

Tokenization has set a new standard for increasingly instantaneous, cheap, and universal asset exchange; the inevitable progression of tokenized assets largely removes the need for investors and even consumers to purchase cash equivalents as a medium of exchange. Traditionally illiquid assets, such as real-estate, will upon tokenization become instantly spendable against an ever increasing and highly liquid universe of tokens, garnering large benefits but also creating hyper intense competition amongst every class and species of investable asset looking to fill the void left by fiat currencies. This leads us to ask the question: Assets live and die by their strengths across a variety of desirable properties. What will determine their survival in a post fiat economy? We argue that asset productivity, scarcity and cash flow will likely be the choice determining factors for a rational economic actor deciding their store of value. In this paper we assess various digital assets from this perspective, including BTC, ETH, and LINK. We then predict what role each of these assets will play in this uncertain future.

Contents

1 The DeFi Matrix

Markets invariably emerge wherever money is found. Bitcoin has pioneered a form of money truly cryptographic in nature, and thus from Bitcoin there has emerged the first truly cryptographic markets, complete with all of the guarantees cryptographic money implies. Put differently, blockchain technology has mathematically recreated the *trust infrastructure* underpinning financial markets: every blockchain supporting tokenization has become an independent alternative for speculators to the NYSE, NASDAQ, The Moscow Stock Exchange, the NEO or the Frankfurt Exchange. To discuss tokenization we first articulate this, that blockchains have mathematically generated the *trust* to meaningfully enable the creation of permissionless and globalized token *markets*, or *token exchanges*.

Blockchains are trustless, extensible, frictionless, constantly accessible, global, transparent, and completely permissionless by their cryptographic nature. Token markets, however, exploit a benefit of blockchains not discussed often – the generality of the strong guarantees of cryptographic trust. Tokenization is a form of digitization, unique in that it is digitizing assets specifically into the securely tradeable cryptographic form suitable for exchange in blockchain markets. Digitized assets necessarily inherit the trust properties and scope of the platform they are created upon. Thus, due to the generality of blockchain trust, tokenization is the most accessible and general form of meaningful asset digitization. Any market can be meaningfully bootstrapped via this process, in the same sense that the NASDAQ first meaningfully created a market for non-physically settled digitized stocks. A tokenized asset is distinctly different than a digitized asset in that it inherits the very broad trust infrastructure of a blockchain, whereas simply digitized assets are *limited* by the legal and infrastructural boundaries of the specific traditional market they are digitized to trade on top of. For instance, NASDAQ stocks cannot be meaningfully represented to trade on Amazon or other online retailers, but tokenized stocks could be traded against tokenized consumers goods, for example. Tokenization has the potential to connect a potentially unbounded array of digitizable assets.

So far, we have already seen this generality allow users to bootstrap markets de novo, such as “Defi”, NFTs, and the myriad attempts to produce digital real estate in so called meta verses. In time, the financial and trust guarantees provided by token markets will simply force the majority of digitized assets to be assimilated into these token markets – into what is effectively one unified cross chain global exchange and liquidity pool. Stocks, bonds, cars, real estate, fiat currencies, insurance etc. – all will be tradeable and ready to be programmatically morphed into the infinite array of other investments on this exchange at minimal to no cost. Balaji Srinivisan termed this global market “The Defi Matrix”. We like the name. The Defi Matrix is inevitable and has deep implications for the world.

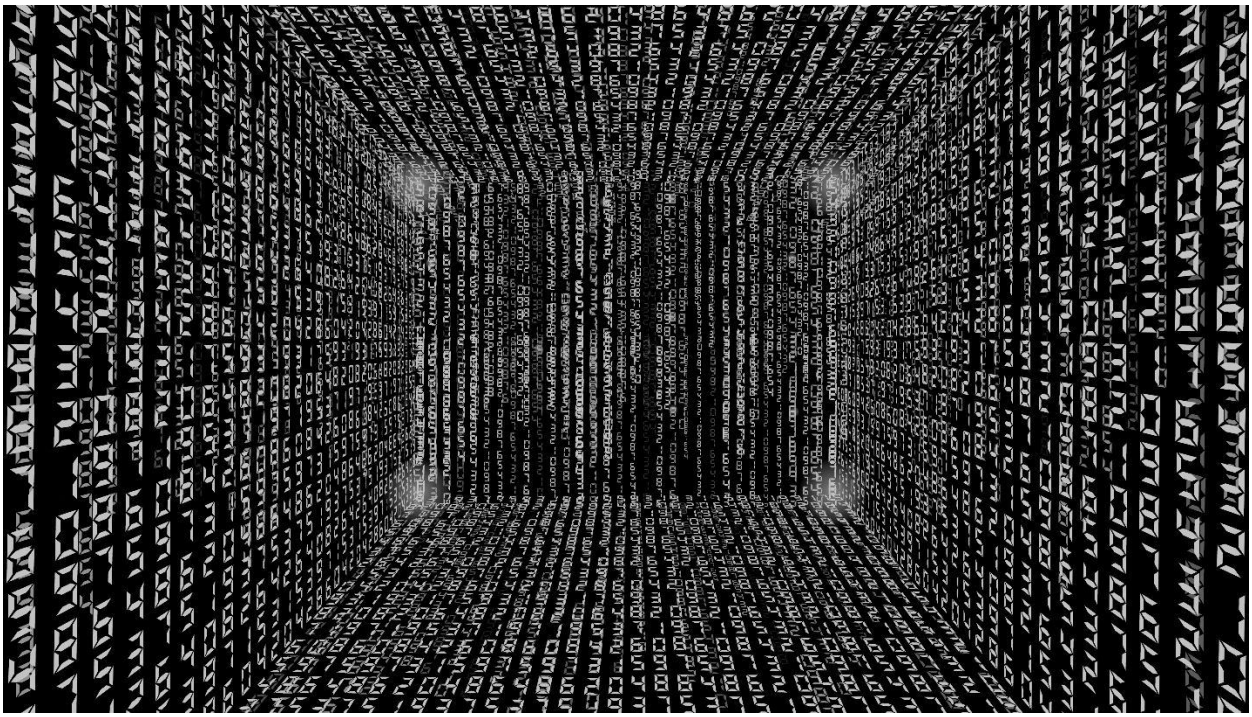

Figure 1 - The DeFi Matrix

The most relevant to our concerns is the minimization or possibly elimination of fiat as a medium of exchange. Every possible market will be bootstrapped, and every token (and thus every asset) will in time become a tradeable asset. What this means is there will exist a clean orderbook for any two tokens, controlled by decentralized and trustless aggregators that find cost minimizing routes through highly liquid intermediaries for investors and consumers alike. Markets that currently do not even exist today will exist with seemingly infinite liquidity (Mortgages/Starbucks Loyalty Points). The cost minimizing route will be defined, amongst other variables, by the deepest liquidity assets connecting the two trading pairs: there is no guarantee this would need to be through fiat currencies, and people would even get used to pricing assets in terms relative to other assets, or maybe in more concrete notions like terms of energy, or other commodities. Thus, there is strong possibility that investors and consumers will have virtually no requirement to buy fiat as a medium of exchange when participating in these token markets.

The benefits of excising fiat from portfolios is of course familiar to investors. Without the burden of having to acquire fiat for liquidity, investors could hold their entire wealth in assets which appreciate in value, while never exposing themselves to the risk of inflation and degradation of value inherent to fiat currencies. Market volatility can be safely hedged against utilizing a wide array of cryptographically enabled stable coins or assets - fiat will even be facing fierce competition in the market for stability.

In this future, assets will be synonymous with mediums of exchange. Consumers may even begin to forget the distinction between an asset and a consumer good as they are blurred together as mediums of exchange. Therefore, every asset will be in perpetual competition with every other asset to serve the purposes fiat once did. Historically banks, and now central banks, are the only entities capable of creating money because of government backing. These entities provided the trust layer for society to agree on the value of an otherwise intrinsically worthless piece of paper. With blockchain markets, trust is now a resource simply backed by mathematics and physics. Anyone can tap into this to generate a token,

allowing for new and unique forms of money. This implies that just as nations compete for their currency to have dominance over others, various digital nation-states or companies will compete to have stronger tokens than others.

We speculate on which assets could be most able to fill the void left by fiat in the wake of The Defi Matrix. Many will be useless, but some will generate a network effect due to unique properties. Bitcoin, for instance, is unparalleled in its proven censorship resistance and implementation of immutable scarcity. Ethereum 2.0 creates a bond-like fixed income instrument as nodes validate blocks in accordance with Ethereum's consensus mechanism, providing the base layer for smart contract security. Chainlink, a decentralized oracle networks, provides all the services smart contracts need but that Ethereum can't provide (such as external connectivity and off-chain computation), in turn providing immense value capture for node operators who contribute to the network.

2 Bitcoin

Currently the largest cryptocurrency, Bitcoin is considered valuable across a variety of axes: Store of Value, Censorship Resistance/Decentralization, Immutable, Non-Corruptible, Fungible, Portable, Durable, and Programmable. There will only be 21 million Bitcoins, making it a sounder commodity than even gold. Currently there are over 15,000 Bitcoin full nodes: Each one would have to be destroyed to destroy the network. Even then, the full chain history could theoretically be recovered. These nodes are distributed across the world in 96 countries, making it highly decentralized and censorship resistant to any single government's policy stance for or against Bitcoin. Bitcoin's ledger is immutable and non-corruptible (so long the Proof of Work consensus mechanism works). Each coin is fungible and divisible to 100 billionth of a Bitcoin. It can be sent to anyone with an internet connection, its digital nature also giving it infinite durability. Finally, Bitcoin has some basic programmability properties.

On its own, I believe Bitcoin would be the greatest digital asset ever invented. The *problem* is that Bitcoin is not the only cryptocurrency. We believe it falls short to Ethereum and Chainlink among most of these characteristics, including as a store of value. The main characteristic Bitcoin appears to be the winner in is censorship resistance. The Bitcoin protocol is the hardest protocol to change, and the supply schedule is effectively immutable. It is also the most proven and decentralized blockchain. Although we believe other assets will achieve higher market caps than Bitcoin, similar to gold it will have a place in the new financial system.

With that said, we are currently neutral on Bitcoin in the long-term because of some technical problems with Bitcoin's consensus algorithm, Proof of Work.

2.1 Bitcoin Instability Without the Block Reward

The first of these problems is hiding in plain sight. Navigating to the holy text of Bitcoin Maximalists, the title of the Bitcoin Whitepaper defines Bitcoin as electronic cash.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Figure 1 - The Bitcoin Whitepaper

"Bitcoin: A Peer-to-Peer Electronic Cash System". The most fundamental problem of Bitcoin, detailed in *On the Instability of Bitcoin without the block reward*, is that the network does not produce substantial cash-flow to maintain the networks security [1]. The security of Bitcoin comes from the network's Hash Power, which is a measure of the total amount of computer power miners are employing to solve the complex math problems to produce the next block. Whoever produces the block, gets the reward. This is currently the main mechanism to incentivizes miners to provide security for the network, and accounts for over 98% of all Bitcoin Miner revenue. The remaining 2% comes from fees, as all fees from Bitcoin transactions go to miners.

The Bitcoin block reward halves ever 4 years – until it ceases to exist around the year 2140 when all 21 million Bitcoins have been mined. This means the block reward is decaying exponentially towards zero. What happens next? Satoshi postulated that the fees generated by the network from *payments* would be substantial enough to maintain the security of network. This is why the whitepaper is titled what it is – the security of the network has this assumption *built in*. The network is extremely slow, only processing 5 transactions per second on average (with a maximum of around 7). This makes Bitcoin completely unusable as a payment network, and the data supports this claim. Navigating to cryptofees.info, one can see the average fees of Bitcoin are similar to that of DEXs on small alternative layer 1 blockchains.

Name	▼ 1 Day Fees	7 Day Avg. Fees
Ethereum	$39,119,058.38	$42,673,461.70
Uniswap	$6,899,013.89	$3,710,813.37
SushiSwap	$2,417,602.34	$1,334,587.07
Binance Smart Chain	$1,936,454.67	$2,218,417.02
SpookySwap	$1,589,803.02	$689,744.08
Trader Joe	$1,254,142.60	$698,297.22
Aave	$988,093.02	$872,213.45
Abracadabra.money	$868,533.84	$567,378.77
Fantom	$685,967.98	$364,226.51
Quickswap	$538,185.07	$282,201.65
Osmosis	$505,026.55	$366,678.95
Terraswap	$434,365.94	$221,241.60
Avalanche	$389,305.66	$484,126.45
Bitcoin	$380,877.44	$380,748.49
Balancer	$371,910.81	$283,405.49
MakerDAO	$315,255.37	$353,906.18
Compound	$222,865.99	$574,831.47
Bancor	$217,849.86	$101,582.14
Polygon	$180,482.53	$169,092.36
Pangolin	$164,339.22	$95,531.80
Arbitrum One	$147,840.62	$157,040.67
ENS	$66,121.08	$113,429.22
Solana	$54,322.31	$111,426.14

Figure 2 - cryptofees.info top fees across all cryptocurrencies

The Bitcoin Lightning network is attempting to solve the throughput problem so that Bitcoin transactions become scalable, but the problem is that the fees are near 0. Lightning nodes must lock up large amounts of Bitcoin to make meaningful fees. For instance, $1 million of BTC locked up could produce upwards of 1% per year ($10,000). That million dollars could be making upwards of 10% per year by providing collateral to DeFi solutions. There are also similar payment solutions that are just as cheap, but do not require massive amounts of collateral locked up [2]. Due to these problems, the lightning network has relatively no adoption, as only $105 million is locked in lightning nodes. Bitcoin as money and payments would also put it in competition with the government. Even Michael Saylor has changed the narrative of Bitcoin being money to now being digital property, as he understands the regulatory risk if Bitcoin tries to compete with the US Dollar.

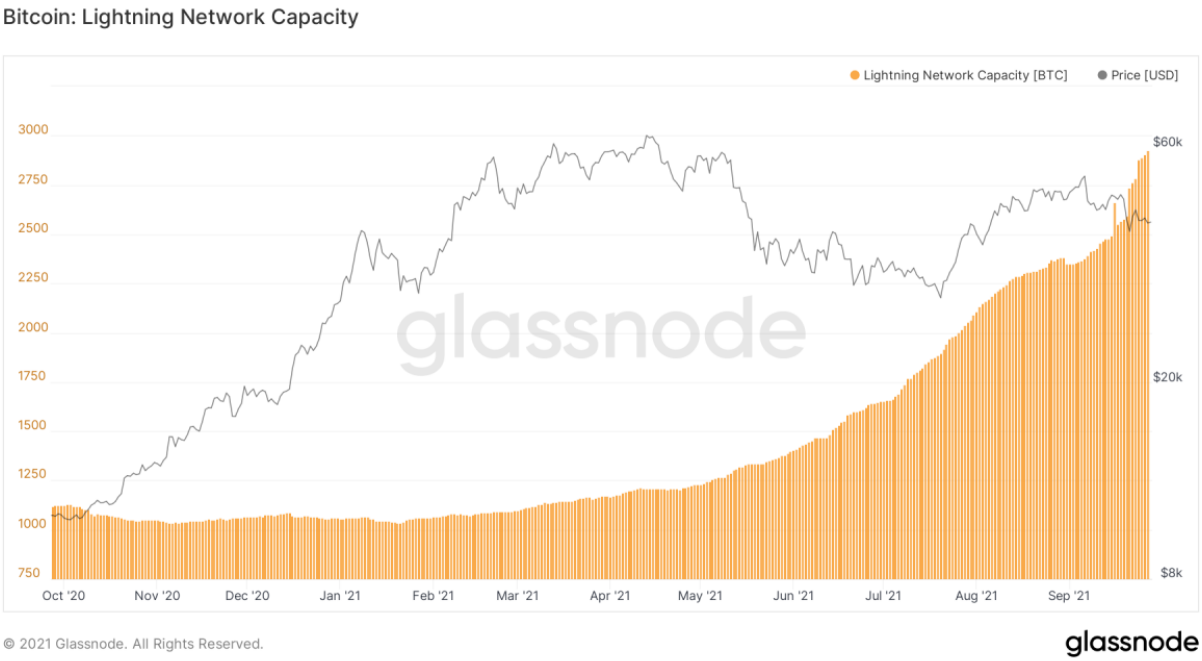

Figure 3 - Bitcoin lightning network capacity is around 3000 Bitcoins, or $105 million.

The other way Bitcoin could theoretically generate cash-flow is by building a layer-2 smart contract chain on the network. A company called Stacks is doing this, and currently has around $0.6 billion in TVL on its network. Note the total TVL on Ethereum is over $150 billion. Stacks security is tied to Bitcoin, but Stacks miners are separate from Bitcoin miners, and have slightly different incentives. Stacks revenue does not equal Bitcoin protocol revenue. Because a Turing complete coding language was not designed into Bitcoin's protocol, finding a permanent solution could prove difficult. As such, there is not only execution risk for Bitcoin to achieving full smart contract functionality, but other protocols (such as Ethereum) have a significant lead on them. As a result, I do not believe smart contracts will lead to significant cash-flow for the Bitcoin blockchain.

These factors lead me to believe that if Bitcoin's price does not keep doubling every 4 years, then it will not have enough hash power to maintain its security. This is because miners must sell Bitcoin to remain profitable. With each halving event every 4 years, miner profits will drop in half, eventually leading to the

network failing as more and more miners will not be able to sustain their operations. Note this is described in great detail in reference [1]. The “2040 cliff” is a common problem acknowledged by some Bitcoiners.

2.2 Energy Inefficiency of Proof of Work

As previously discussed, Bitcoin Miners utilize computational resources to secure the network via the Proof of Work consensus mechanism. This process is highly energy intensive, as current estimations place Bitcoin’s energy usage at 0.5% of global energy expenditure.

This is a highly nuanced problem as well, because in isolation I do not believe Bitcoin to be a waste of energy. If Bitcoin was the only means to achieve a digital, censorship resistant, scarce form of money, then this energy expenditure would be well worth it. The problem, once again, is that there are cryptocurrencies that use more efficient consensus mechanisms. Ethereum, for instance, will soon upgrade to Proof of Stake, which will drop its energy usage by around 99.95% [3]. Proof of Stake nodes can run on any basic cloud compute infrastructure, such as AWS. There is no additional hardware or energy requirements to participate in consensus – just a capital requirement in the form of owning Ether.

Bitcoiners argue that the Proof of Work Energy problem is leading to a future of clean energy, as the cheapest energy will always be that of renewables. Although this is true, estimates put its renewable energy mix at a maximum of 56% [4]. I have heard this number as low as 35%. Regardless, it doesn’t matter either way. Even if we assume that Bitcoin’s energy mixture was perfectly renewable at 100%, this energy can be considered wasted by the exact delta between the energy expenditure of Proof of Work vs. Proof of Stake, i.e. a 2000x difference. This extra energy that must be used represents a massive opportunity cost for other services that could add value to society.

Although there are some short-term benefits to Proof of work, such as using would be flared gas to power Bitcoin mining facilities or consuming excess electricity to stabilize energy grids, these are not significant long-term solutions. With advances in energy storage technology, the potential energy in flare gas could be stored for later use. Similarly, flare gas can be utilized to create cloud compute centers to run Proof of Stake validator nodes as well. Although helpful for consuming excess grid electricity, it is not a perfect long-term solution. There is the concern that Bitcoin miners are not regulated properly and that they will continue to negatively impact customers by consuming electricity during peak demand hours and potentially creating energy shortages. Personally, I would not want to rely on politicians to create effective regulation here, where wealthy Bitcoin farmers could easily “lobby” them to allow them to keep their ASICs on at all hours of the day. The best solution here is to store excess grid electricity in energy storage solutions, such as dams or novel energy storage solutions. One such example is Energy Vault’s gravity and kinetic energy based, long-duration energy storage products.

Ari Juels, currently Chief Scientist of Chainlink Labs, coined the term Proof of Work in a 1999 research paper [5]. In his testimony at The Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, he concluded his opening statement with: “The bitcoin community deserves our deep gratitude for introducing blockchain to the world, but we have far more energy efficient alternatives than proof of work.” [6]

2.3 Bitcoin Provides no Cashflow for Holders

On another note, productive assets, such as Ethereum or Chainlink, will produce cashflows for owners while maintaining similar or better store of value properties. All else equal, rational economic actors will

prefer to hold these assets to Bitcoin in nearly all economic conditions. On a relative basis, I expect them to perform better over time than Bitcoin, eventually leading to much larger market caps. I will discuss these assets further in later sections.

2.4 BTC Conclusion

Although I am bearish on Bitcoin on all time frames against other digital assets such as ETH and LINK, I am bullish in the short and medium term versus the US Dollar, and neutral in the long term. Bitcoin is effectively digital gold, the purest form of collateral, and I expect its market cap to reflect that. Bitcoin also has unique censorship resistance properties that no other cryptocurrency has. Although it won't be the best store of value, *it will have the most predictable supply schedule*, and there is immense value in having certainty as an investor. Gold is around a $10 trillion market cap asset, whereas the combination of stocks, bonds, and real-estate are more than $500 trillion. I believe the ratio of Bitcoin to fixed-income, stocks, and productive assets will be similar to this.

Assuming Bitcoin reaches a market cap of $10 trillion, this would imply a price of around $500 thousand a token. Note that would mean the price doubling somewhere around 3-5 times. In 3 or 5 halvings, approximately 10-22 years from now, the price would have to reach this value for security to be maintained. After that, the price would have to continue doubling in order to maintain security. As stated earlier, I have a hard time believing the price would extend beyond this point. Almost ironically, it would appear Bitcoin would need to change its monetary policy and implement a permanent inflation rate in order to maintain security at this point. As such, I remain long-term neutral on Bitcoin until I see evidence of the fee problem being solved. I think for the next decade it is a strong hold due to the censorship resistance properties and strong network effect by being the first mover. Beyond that, I think its relevance will fade over time. The Proof of Work energy problem is nothing to scoff at, either. Although Bitcoin is the most insulated from security regulation risk, I believe it has the highest regulation risk with respect to environmental concerns.

Finally, there is an investor psychology aspect to this too. New users want to get into tokens on the ground up, where they believe they can become rich. If Bitcoin is already in the $100s of thousands of dollars per coin, how much upside does it really have? Once all store of value assets are tokenized, Bitcoin is going to face fierce competition from other sources, specifically real-estate. If Bitcoin's market cap is already $10 trillion, would you rather put your money into a tokenized Malibu real-estate trust, or multi-family property real-estate for the states of Texas and Florida, which also return cash-flows from renting costs? Although these can be viewed as inferior assets due to tax reasons, upkeep costs, etc., if one can get into these projects on the ground floor the upside will greatly outweigh these downsides. Regardless, I believe Bitcoin is a crucial part of every investor's portfolio.

3 Ethereum

In order to have a fair and transparent financial system, solving money is just the first step. The next is creating an internet of contracts which force transparency and eliminate counterparty risk, such that events like The Great Financial Crisis cannot happen again. The first Turing complete smart contract protocol, Ethereum expands upon Bitcoin by enabling the creation of programs that run on top of the ledger to programmatically move tokens. This enables applications to be built such as DeFi, NFTs, and stablecoins. If Bitcoin is a calculator keeping a simple tally of who holds which coins, Ethereum is a global computer capable of keeping track of state, storage, and tokens across thousands of applications running in parallel.

“Ethereum was designed to be a decentralized global supercomputer impervious to third-party control or censorship. Given that every single operation that takes place on the Ethereum network requires some amount of computational power, this emphasis on decentralization requires an alternative model for facilitating on-chain transactions and incentivizing network use. In order to address these challenges, the developers of Ethereum created ether (ETH), the blockchain’s native coin, to power the network.” -Gemini

The implications of an internet of contracts which replace many industries today cannot be understated. Smart contracts aim to disrupt deca-trillion-dollar industries (finance, insurance, global trade). The focus of this paper is not on the value proposition of smart contracts, but instead the assets which aim to capture value from this technology. For more research on the impact of smart contracts, please refer to other Abstraction Capital insights, or articles online which detail this impending shift.

Currently DeFi on Ethereum has around $150 billion locked in applications, proving there is demand for such applications. This demand has generated an enormous amount of protocol fees in the short history of Ethereum. Every computation on the Ethereum Virtual Machine must be paid for in Ether. As such, every application built on the network expands the demand for ETH. Hence, Ethereum is a cashflow monster. In Web 2.0 the base layer (TCP/IP, HTTP/S, etc.) accumulated little to no value. The applications built on top (Facebook, Google, etc.) were the winners. In Web 3.0 this dynamic inverts. Although applications will be tremendously successful, their success necessarily indicates the base layers success. As the number and size of applications grow, so does the underlying blockchain.

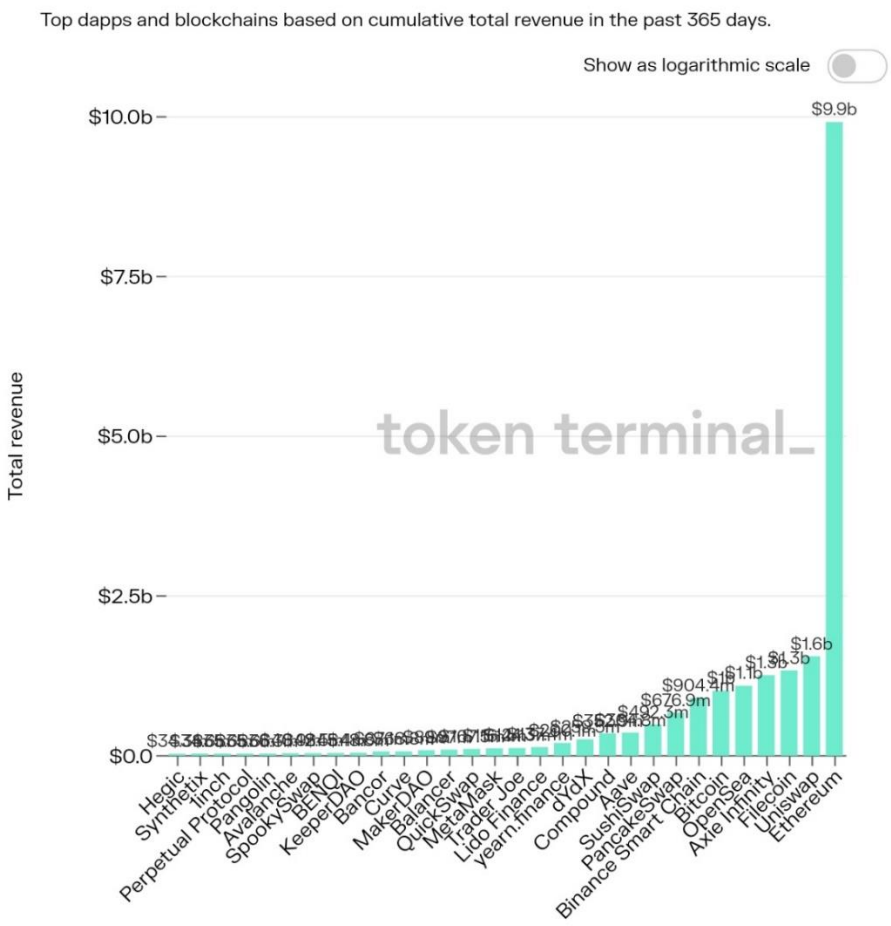

Figure 4 - Ethereum generated nearly $10 bil in revenue in 2021 (taken January 1, 2022)

Ethereum is currently in the process of upgrading to version 2.0. This will transition the network from Proof of Work to Proof of Stake, which (as discussed prior) will make the network significantly more environmentally friendly. Although there are a few theoretic arguments about the security of Proof of Stake, in practice Proof of Stake networks have experienced no such problems. This has been mostly proven out because Proof of Stake networks secure $100s of billions in value and have yet to be hacked – any potential hacker could walk away with billions, creating massive incentive to break Proof of Stake. It is also important to note that every major blockchain today – Solana, Avalanche, Terra, Fantom, Near, etc. – chose Proof of Stake over Proof of Work because they understood it to be fundamentally as secure.

Proof of Stake also offers better decentralization properties because *anyone* with a laptop and an internet connection can run a validator node. One does not need millions of dollars to construct a mining facility to participate in consensus. Bitcoiner's argue that Proof of Stake hurts decentralization because the largest stakers earn more ETH – "the rich get richer". Although this is true in absolute terms, the relative ownership of the network of each participant always stays the same because staking rewards are earned relative to network ownership. If you own 1% of the network and always re-stake your Ethereum, you will *never* own less than 1% of the network[i]. If larger entities sell ETH holdings to cover larger tax liabilities, your network ownership will increase over time. Larger entities distributing coins to invest in other assets is a common trend we have seen in both Bitcoin and Ethereum. Millions of individuals staking ETH on

computers, laptops, and phones across the world is more decentralized than the 4 mining pools which own more than 50% of the hash power on the Bitcoin network.

The only argument Bitcoin has at this point is the Lindy Effect – Bitcoin has proven Proof of Work to be highly secure because it has survived more than a decade. As more time passes and Proof of Stake networks continue to survive without hacks, though, it will be harder to defend Proof of Work. There is an abundance of material on this topic, and as such this paper will not go more in depth on this. The key takeaway is that in theory Proof of Stake is better across various axes and has so far proven that out.

Not only has Ethereum chosen to upgrade to a better consensus mechanism than Bitcoin, but the Ethereum token produces cash flow for its holders and has designed a better monetary policy for its token as well.

3.1 ETH 2.0: The Emergence of a Bond-like Instrument

The first phase of Ethereum's upgrade to 2.0 is to establish the Proof of Stake Chain: The Beacon Chain. Once stablished, the Merge will then transpire sometime around Q2 or Q3 in 2022, where the Proof of Work Chain will merge into the Proof of Stake chain. For the Beacon Chain to launch, it required 554,000 ETH deposits. This number was chosen because it would ensure enough validators to maintain the security of the network. With this many deposits, the inflation rate of Ethereum would drop to 0.5%. This is because the network no longer needs miners. Instead, emitted ETH would go to stakers who validate the network. These stakers post ETH as collateral, and risk losing said collateral if they do not validate the ledger honestly. If they do act honestly and correctly validate the network, they get rewarded with ETH. The beacon chain ready and awaiting the merge with over 9 million ETH staked [7]. Although execution risk remains, it is clear Ethereum has the backing of its supporters, as all ETH staked in the beacon chain staking contract is locked until Proof of Stake goes live. I fully expect the merge to go through this year.

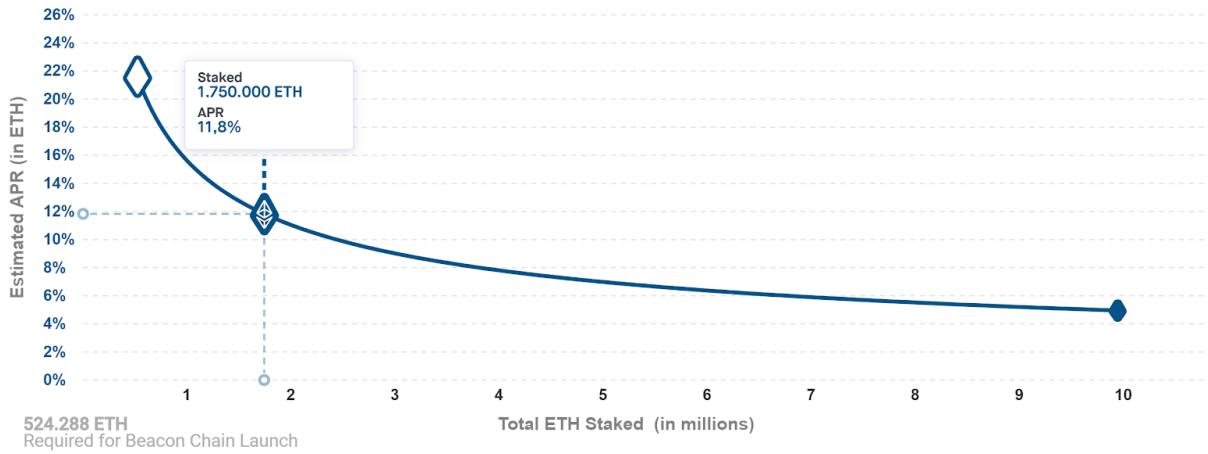

Figure 5 - ETH Staking APY Curve

Currently, the ETH staking APY is around 5%. As more ETH is staked, each validator is called upon less frequently, and hence the APY decreases. The "ETH Yield Curve" is very similar to a perpetual bond, as discussed by Kasumovich and Martinak:

"The ETH-flow from staking can be judged as a perpetual bond. A rise in the confidence of the network and the value of holding ether as the base collateral of the ecosystem leads to a virtuous cycle of lesser

supply and declining yields. Yields are currently trading 5.25% with nearly 8 million ether staked. This is close to 5-year peso bond yields in Mexico for broader market context. At 20 million ether staked to the network – 17% of total supply – yields decline to 4%. A decline in yields to 2% would increase the bond value by three-times from current levels and with deposits of more than 40% of ether supply." [8]

After the merge, it is predicted that ETH yields will jump to 9-12% as rewards will incorporate net transaction (ex-base) fees currently paid to miners. With that said, this will likely drop quickly back to around 5% as more and more ETH is staked. As yields compress, validators may decide to withdraw their ETH to utilize it for other, higher yielding use cases. As the APY increases, though, it will eventually attract stakers back. With projects such as Lido which provide liquid staking, users can withdraw a derivative of the ETH token, stETH, which can be utilized throughout the Ethereum ecosystem. This provides a means for users to gain liquidity for otherwise locked Ethereum [9]. As a result, I expect there to be significant staked ETH, with yields oscillating around 5%.

The result of staking is incredibly bullish for the price. As more ETH is locked in staking, the circulating supply must decrease. With constant demand, price must increase. Because ETH must be utilized to pay for all network services, there will always be demand for ETH. I believe the cash-flow component of Ethereum is simply one characteristic that will make it more desirable to hold than Bitcoin. In the next section, I will describe an upgrade to Ethereum's monetary policy that further extends its advantage.

3.2 EIP-1559: A Smart Contract Protocol with Monetary Premium

Over the years, Bitcoin has settled on the narrative of being digital gold. The network rarely upgrades, and that is by design. The more boring Bitcoin is, the stronger its case to be pristine collateral, beyond the control of any individual. Although Bitcoiner's see this as a feature, I see it as a both a feature and a bug. It is a feature, because one can be (nearly) certain Bitcoin's monetary policy will never change. It is a bug because it leaves the protocol defenseless from competition.

Up until 2021, Bitcoin had a stronger monetary policy than Ethereum, as it was less inflationary. Currently the base inflation rate of Ethereum is around 4.5% and is asymptotically approaching around 1% over time. This permanent inflation was designed into Ethereum to ensure it could retain its security far into the future. Clearly the Ethereum developers understood the problem I discussed in Section 3.1 (the instability of Bitcoin without the block reward). Regardless, its inflation rate was much higher than Bitcoin's. This all changed with EIP-1559.

The core Ethereum developers proposed Ethereum Proposal Improvement 1559 in April of 2019, which went live in August of 2021. EIP-1559 changed Ethereum's fee market mechanism, getting rid of the first price auction as the main gas fee calculation. Now, there is a discrete "base fee" for transactions, with optionality to include a miner "tip" to get your transaction processed first. The base fee is permanently burned. This means that the total supply of the network decreases in proportion with its usage. Already more than 1.6 million ETH has been burned – over $4 billion dollars-worth [10].

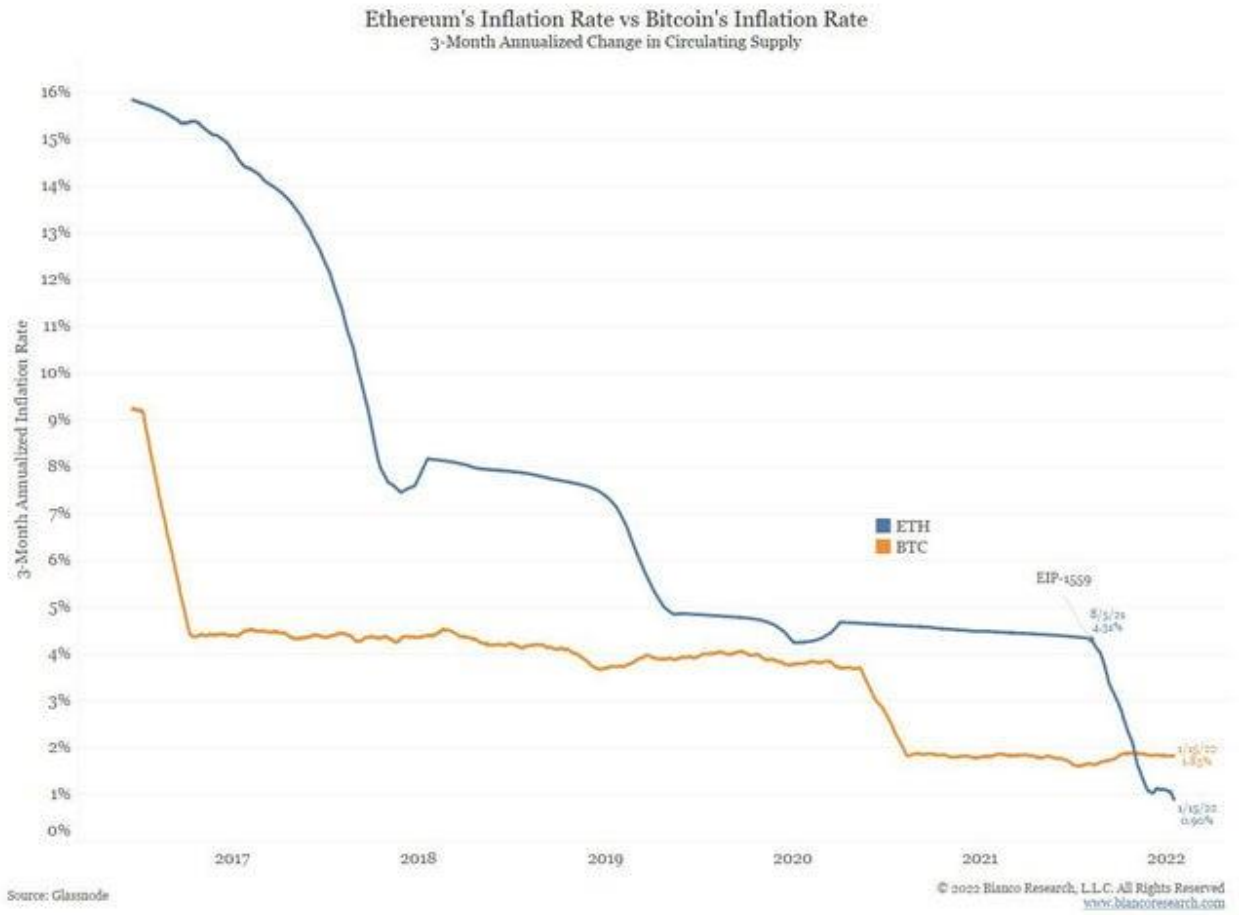

Figure 6 - ETH vs BTC inflation rate

ETH has a lower inflation rate than Bitcoin post EIP-1559. Although Bitcoin's inflation rate will continue to halve into perpetuity, eventually hitting 0%, Ethereum is set to become deflationary after the Merge happens. This is because ETH 2.0 will decrease the base inflation rate further.

ETH validating	Max annual issuance	Max annual network issuance %	Max annual return rate (for validators)
1,000,000	181,019	0.17%	18.10%
3,000,000	313,534	0.30%	10.45%
10,000,000	572,433	0.54%	5.72%
30,000,000	991,483	0.94%	3.30%
100,000,000	1,810,193	1.71%	1.81%

Figure 7 – ETH Validator Issuance. Current ETH supply is around 118,000,000

With a base level of inflation hovering around 0.5%, as the Ethereum network scales it will become more deflationary because more usage means more fees burned. Once deflationary, Ethereum will be a scarcer asset than Bitcoin.

Bitcoiners most common critique of ETH being a better store of value is that just as easily as the monetary policy changed before, it could be changed again – except the next change could harm the asset (such as making it more inflationary, etc.). Although theoretically this is possible, what incentive do the core Ethereum developers and larger community have to change it? It is in Ethereum's best interest to keep its current monetary policy, and it will become increasingly more difficult for the chain to approve upgrade proposals as it further decentralizes. Ethereum is more decentralized than ever, with more active addresses than Bitcoin as of June 2021. It is also untrue that Bitcoin can't be changed. It took 3 years for EIP-1559 to go through, whereas it took 4 years for Bitcoin's Taproot upgrade to go through. Although it is inarguably harder for Bitcoin proposals to pass, as discussed earlier problems with Proof of Work from an environmental and technological perspective could eventually force the developers to eventually change the protocol in a meaningful way. Ironically, Bitcoin's biggest perceived strength could become a narrative nightmare if they are forced to change the monetary policy. Ethereum also has a robust process for making any changes to the protocol.

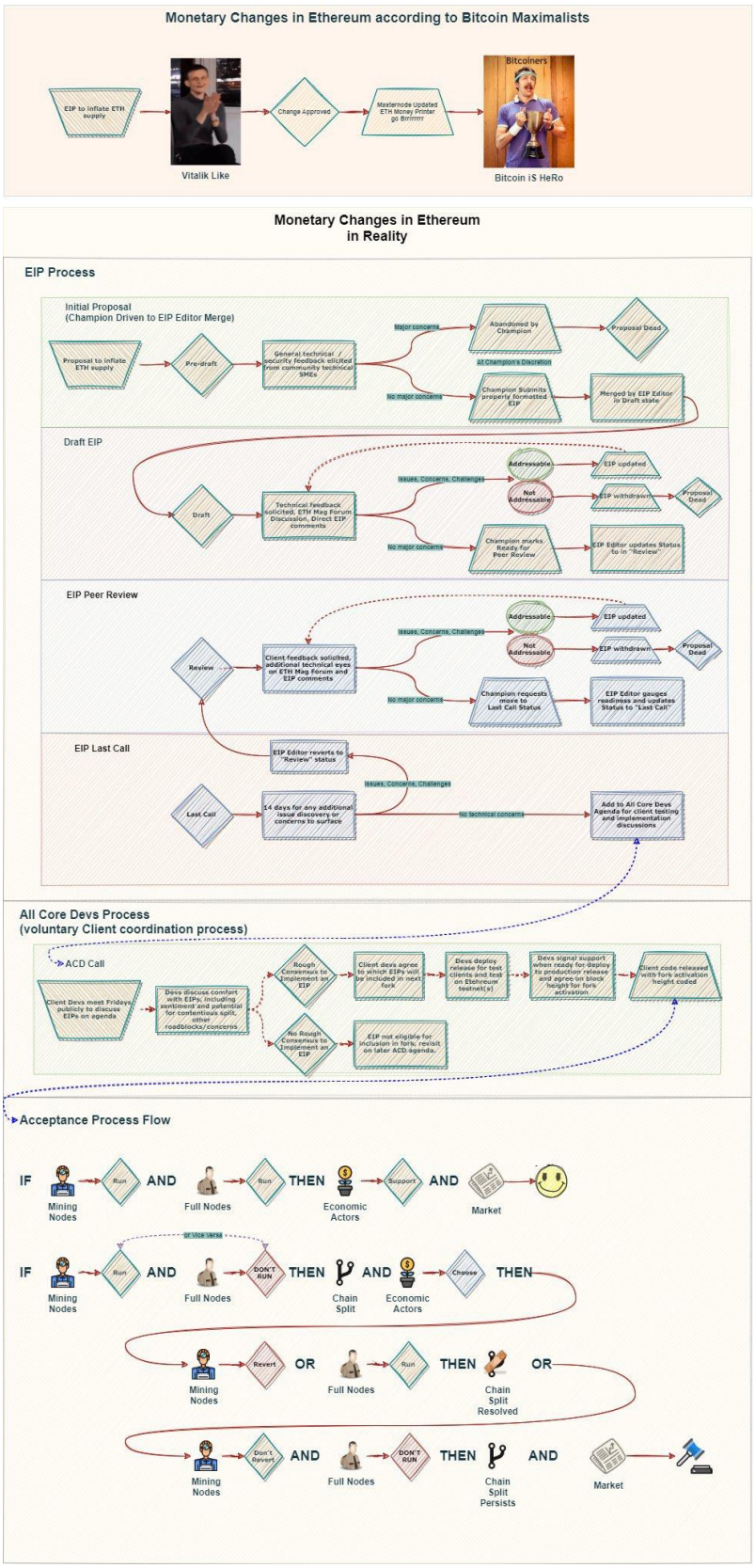

Figure 8 - EIP process flow is a highly redundant process with checks and balances

Ultimately, with a world of thousands of competing currencies the ability for a chain to upgrade is more valuable than its ability to stay the same. There is an analogy to this in legacy markets which supports my point. Even though any company can technically perform a dilutive Secondary Offering and issue more shares, stocks remain much more valuable than gold in terms of relative market cap. This is because companies understand incentives, and do not want to destroy the value of their stock. The same holds true with blockchain protocols. Ethereum is now mathematically sounder money than Bitcoin. There is no debate – the inflation rate is lower and will likely remain lower into perpetuity so long there is demand for Ethereum based smart contracts. Although execution risk remains, I believe on a 3–5-year time horizon the sentiment shift to ETH being sounder money than Bitcoin is inevitable.

In conclusion, due to the fact that ETH is scarcer than BTC and also produces cashflow for the holder, I would argue it will be a more desirable asset to hold. With that said, ETH has competition from alternative L1 protocols, as well as potentially parasitic L2 protocols.

3.3 Trust-Minimized Computation is a Deflationary Resource

Ethereum cashflow is predicated on the number of transactions that take place on the network, as well as the cost of those transactions. In the next few sections, I will discuss why the cost of those transactions are set to reduce drastically. With that said, increased usage of the network should offset the drop in costs.

3.3.1 Chain Wars: Competition will Drive Down Costs & Dilute Market Share

As an increasing number of Layer 1 and Layer 2 chains are created, the competition for users will only grow. The product users desire is trust minimized computation, or blockspace (I will use these terms interchangeably throughout this section). Just as any resource, the cost of trust minimized computation will decrease over time as competitors fight for users and technological progress is made. We have seen this play out with the first three stages of compute: Mainframe/personal computers, Web-based enterprise applications, and then cloud/mobile computing. With respect to cloud computing, “Byrne et al (2017) created price indices of the various cloud services offered. They estimate that cloud processing prices fell by about half between 2009 and the end of 2016, while storage prices fell between 70 and 80 percent during that time period.” [12]

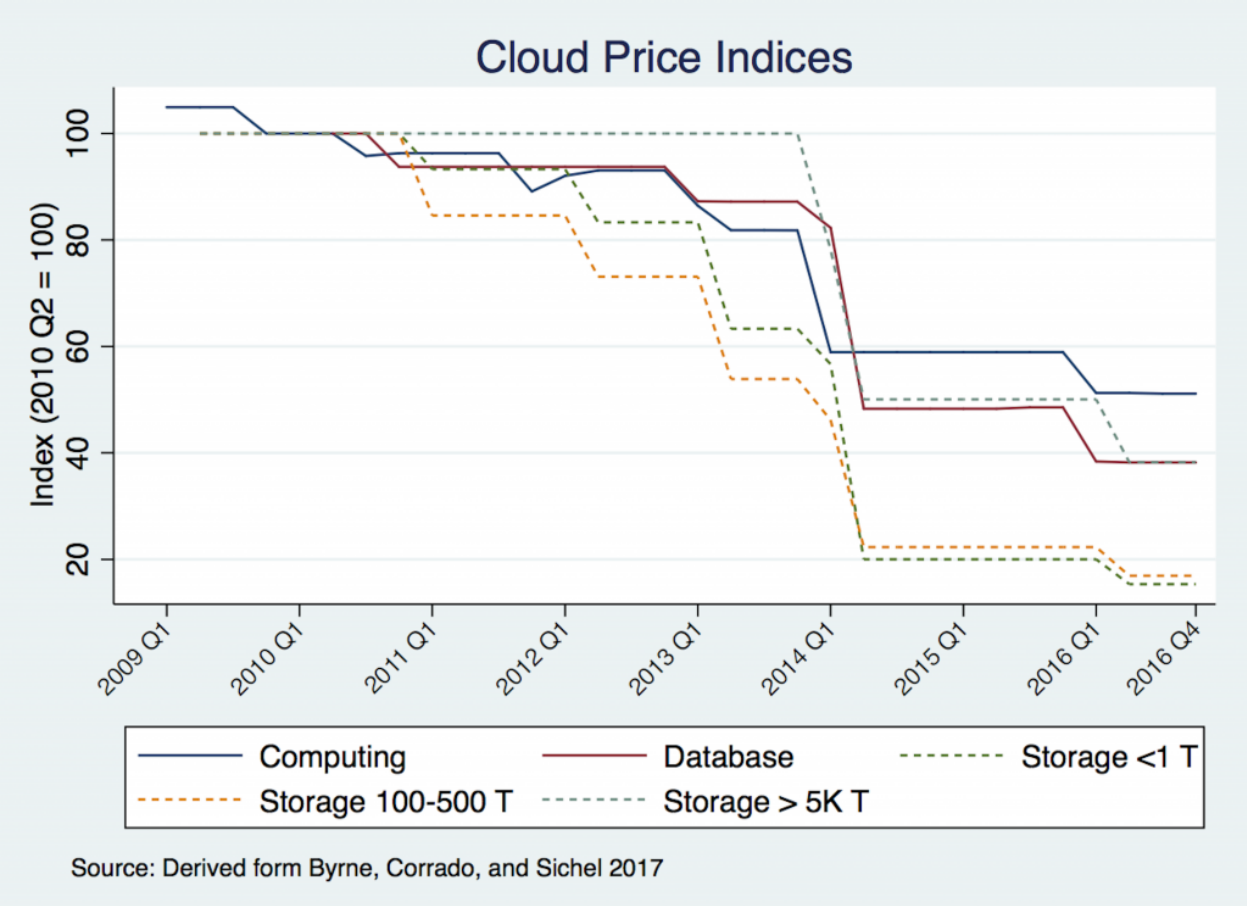

Figure 9 - Drop in cloud prices over time

AWS, Microsoft Azure, Google Cloud, and others compete to provide cloud infrastructure. The competition has driven costs down for end users – it only costs around $90/month to spin up an AWS instance. Each user has various strengths and weaknesses as well. AWS, for instance, has become a major player in AI, database, and machine learning serverless deployments, while Azure is the preferred enterprise SaaS platform.

Figure 10 - Cloud Infrastructure Competitors

I foresee a similar dynamic with blockchain protocols. With the rise of alternative L1 protocols in 2021 such as Binance Smart Chain (BSC), Polygon, Solana, Avalanche, and Terra, new alt L1s gaining hype such as Polkadot, Cosmos, Fantom, and Near, and highly performant enterprise chains such as Hedera Hashgraph, Algorand, and Oasis potentially on the horizon, it is becoming increasingly clear we will live in a multi-chain world. To me, that is no longer a debate. The true debate lies in how capital will be distributed amongst the chains. As nearly all economic games in life, I believe the relative value of chains will follow a Pareto distribution in terms of market share, where there are a few large chains bifurcated by use-case and geography, with a fat tail of smaller chains for hyper-specific use cases or geographies.

2021 made it clear that there is demand for cheap blockspace. After Ethereum fees became as high as $100 dollars for a token swap, ETH lost significant market share while users flocked to BSC, Polygon, Solana, and Avalanche to perform cheap transactions. For retail users who are trading small positions or flipping NFTs, the security offered by Ethereum was simply not necessary – the only thing is achieved was completely priced out new users. It is important to remember decentralization is a spectrum and is not necessary for every transaction. This is why I believe a “trust-minimized computation curve” will begin to develop over time.

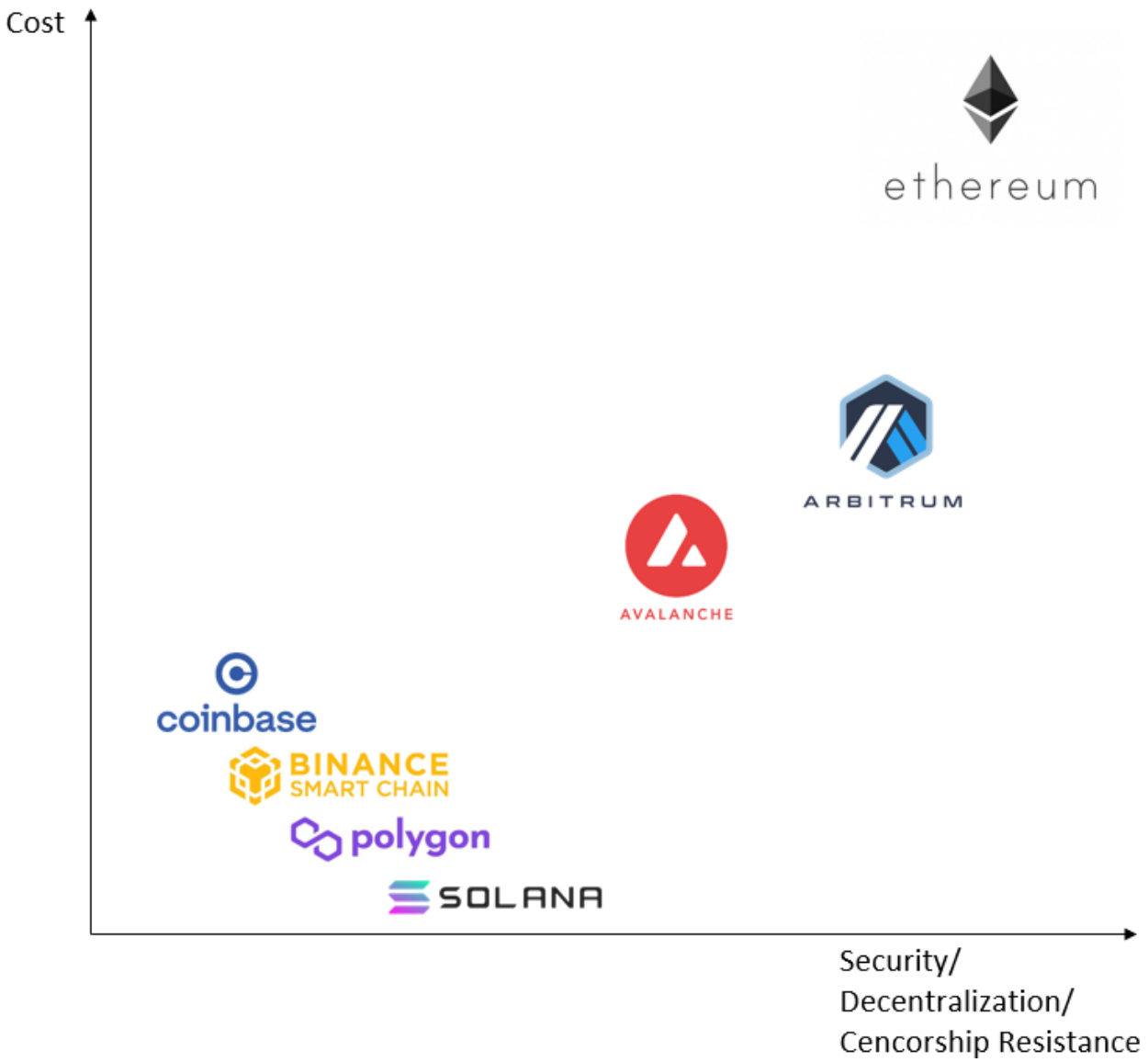

Figure 11 - Trust-minimized computation curve. Shown are some popular companies or protocols. I attempted to be fair with respect to historical transaction fee costs.

This figure gives one the general idea of this concept. One can think about security like insurance. Although one is more likely to lose money transacting on less secure chains, considering the lower costs it is still more profitable to utilize them for retail users. For hedge funds trading billion-dollar derivatives, utilizing the ETH main chain or an Ethereum L2 rollup such as Arbitrum will likely be the choice.

Although Ethereum is the most secure chain, what does that actually mean? Every chain has a cost to attack it, which is dependent on the hash power of the network (in the case of Proof of Work protocols), or the cost to purchase a majority of network tokens (in the case of Proof of Stake protocols). Rigorous ways to calculate the cost to 51% attack or to DDOS spam and censor a network will emerge over time, ultimately leading to a consensus of best practices that will guide users to the most performant chain that retains enough security for the amount of value they plan to transact.

Currently, do any of these chains truly pose a threat to Ethereum? I would argue it is too early to tell. Although Layer 1 protocols have performed brilliantly in 2021, I believe this has mostly been due to speculation. Once Ethereum fees priced out retail users, what we effectively saw were developers copy-pasting code from popular Ethereum dApps to the alt-chain of their choosing. Binance chain needs a DEX? Let's fork the code, call it Pancake swap, and drop fees many orders of magnitude. Avalanche needs one too? Let's fork the code and call it Trader Joe. This same process was done with lending protocols, NFT marketplaces, yield farming protocols, etc. The crypto money ball chased the hot new dApps on BSC, then Solana, then Avalanche, etc. I would argue other than fees (which have come at the cost of decentralization), there isn't really a differentiating factor these other chains offer…yet. There will be some dApps that can only work on high throughput, low-cost chains, and I am exciting to see what starts to get built. Similarly, some blockchain games might require very high throughput, and as such be built on a chain like Solana. These chains are now incredibly capitalized, and with growing developer communities. It is up to these chains to fund developers to create unique use cases that will cement their place in the multi-chain future.

3.3.2 Parasitic Endgame? ETH Scaling is Rollup Dependent

In a somewhat recent blogpost, Vitalik Buterin described the path by which Ethereum will attain scalability. Ethereum is going to become a security/consensus and data availability layer, while L2 rollups handle execution [11]. This modular architecture could allow Ethereum to scale to millions of transactions per second at fractions of a cent by the end of the decade. Not only will it have the best security, but it will compete in terms of transaction speeds. As a combination, I ultimately do not believe any Monolithic blockchain will be able to compete on the security front – monolithic chains are subject to the blockchain trilemma of having to choose between security, decentralization, and scalability. Lucky for other chains, L2 rollup technology is applicable to any blockchain, not just Ethereum. As a result, I agree with Vitalik's assessment that all blockchains will converge on L2 solutions or the practice of isolating computation from the rest of the blockchain.

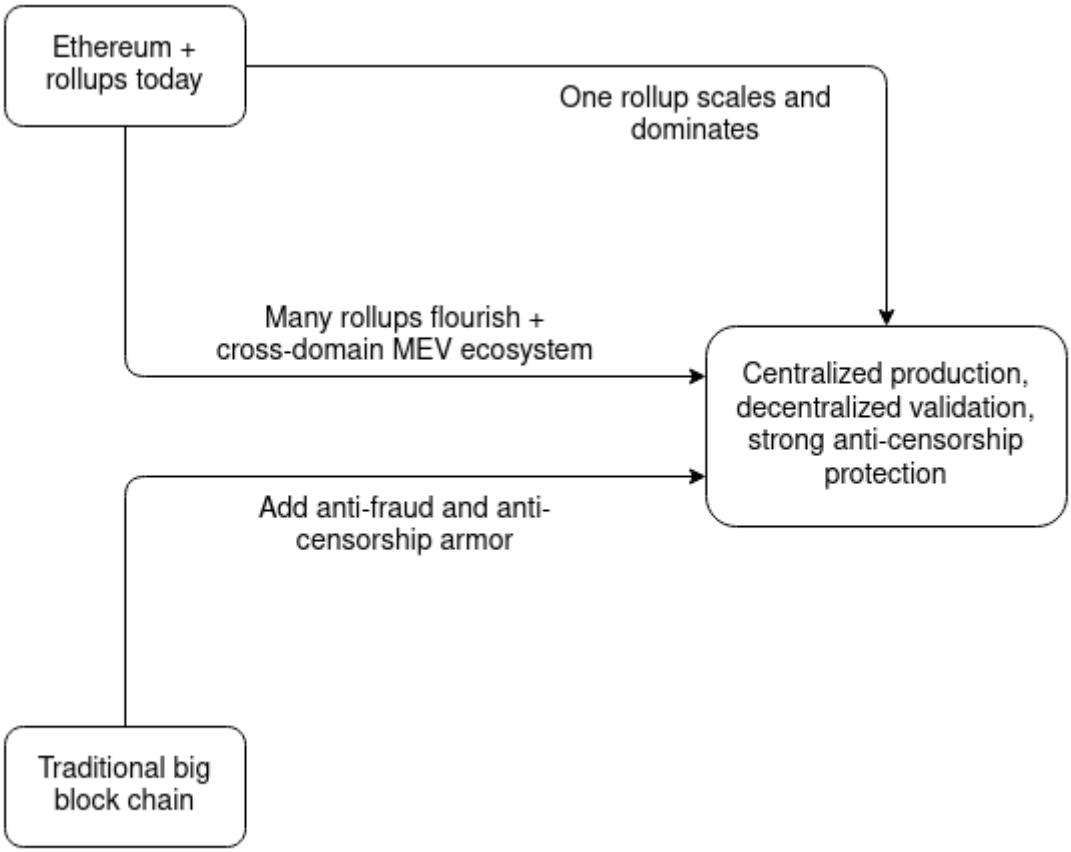

Figure 12 - Vitalik: All paths lead to the same place

Emin Gün Sirer, founder of Avalanche, has identified an issue with modular computation that is handled by a different protocol than the base layer:

“Another problem with L2s is they bring no value to the underlying chain. They are all parasitic by nature and inherently. Why? Because essentially, they are there to come and cannibalize any value on the chain and move it elsewhere. They are just another blockchain.”

He then uses an iguana analogy that some male iguanas develop female markings as a reproductive strategy, so that they do not have to fight male iguanas but can instead sneak onto a male iguana’s rock and mate with the female without being noticed as a rival.

Figure 13 - ZK Sync, Starkware, Arbitrum, and Optimism cannibalize ETH's value, an Emin Gün Sirer analogy

Although biased from his position running Avalanche, I mostly agree with Sirer on this point. The problem for Ethereum is that although rollups pay for Ethereum's security, the do not necessarily share protocol fees with Ethereum. Arbitrum, Optimism, ZKSync, and Starkware all plan to launch tokens (not confirmed, but this is obvious). As Vitalik describes in Endgame, nearly all computation is going to be moved to rollups. That means the only fees the base layer will be collecting are from rollups posting fraud or validity proofs to the mainchain, in the case of optimistic and ZK rollups respectively. This is where I disagree with Sirer slightly. L2s are not completely parasitic because they still have to pay fees to the main chain for security. Due to the massive number of transactions that are likely to take place on L2s, there are going to be thousands of unique rollup chains created for specialized purposes. All of these chains will be paying gas fees to the Ethereum main chain. Recently, the Arbitrum Sequencer was the highest gas consumer on the Ethereum network in a 24-hour period, paying nearly $65,000 in fees.

Top 50 Gas Spenders (Sending Accounts that pay a lot of Gas)

Rank	Address	Fees Last 3hrs	% Spent 3hrs	Fees Last 24hrs	% Spent 24hrs	Analytics
1	Arbitrum: Sequencer	$24,074.46 (8.06 Eth)	1.95%	$64,714.83 (21.67 Eth)	0.59%	
3	Coinbase 4	$6,708.31 (2.25 Eth)	0.53%	$58,073.69 (19.44 Eth)	0.48%	
2	Ethermine	$6,708.59 (2.25 Eth)	0.56%	$54,272.17 (18.17 Eth)	0.53%	

Figure 14 - Highest Ethereum Gas Users - March 22nd on https://etherscan.io/gastracker

Although Arbitrum and other rollups are paying high gas fees right now, these are set to reduce drastically. Eventually, rollups will have the capacity to compress thousands, and eventually millions of transactions into single proofs. After just EIP-4844, the cost for rollups to settle on Ethereum will drop over 100x [24].

	Before EIP-4844 (Send ETH)	Before EIP-4844 (Swap tokens)	After EIP-4844 (Send ETH)	After EIP-4844 (Swap tokens)
Boba Network	$0.06	$0.40	$0.0006	$0.0040
Loopring	$0.07	$0.69	$0.0007	$0.0069
zkSync	$0.09	$0.22	$0.0009	$0.0022
Polygon Hermez	$0.25	-	$0.0025	-
Optimism	$0.37	$0.54	$0.0037	$0.0054
Arbitrum One	$0.53	$0.74	$0.0053	$0.0074
Data sourced from L2fees.info		March 17, 2022		

Figure 15 - Rollup transaction fees post EIP-1448 [26]

After Danksharding and further rollup upgrades, there is expectation fees will go down even further, possibly 1000x. As Polynya, and expert on L2 protocols, says, "It's going to be negligible cost for rollups to settle on Ethereum, and the DA space will continue expanding progressively with Danksharding post-4844. Ethereum will simply fade into an invisible security provider for rollups."

Although costs are going to decrease to nearly 0 for a simple wallet transfer, if the world is indeed powered by smart contracts in a decade there is the potential for millions of transactions per second. I think it is reasonable to assume a slightly deflationary or inflationary supply into perpetuity, so long ETH + L2s remains the highest security per unit cost solution for smart contracts. Ultimately, Ethereum failed to scale fast enough with plasma, sidechains, or sharding. Where Sirer is correct is from a business standpoint, the potential value capture of Ethereum has been impacted immensely by its failure to scale, and now being reliant on L2s. In terms of the performance of a modular Ethereum and costs for end users, I see no problems.

3.4 ETH Conclusion

The ability for Ethereum to generate cashflow has enabled it to have a stronger monetary policy than Bitcoin. This is why productive assets, in my opinion, are set to be the best type of money in the digital age. The burning of base gas fees via EIP-1559 can be viewed as a perpetual stock buyback which ties the overall usage of the network to the monetary value of the token. Ethereum 2.0 and Proof of Stake creates a bond-like instrument which is accessible to all users – not just those with massive mining facilities. It will also lower the inflation rate, setting the stage for ETH to become deflationary after the Merge. With Proof of Stake a more energy efficient and viable alternative to Proof of Work, I see no reason why economically rational actors would hold more BTC than ETH. As stated in Section 3.4 I do believe there is a place for BTC (just as there is a place for gold), but simultaneously believe ETH will drastically outperform BTC in the long-run, and without any of the potential security vulnerabilities.

Although I am bullish on ETH/BTC and believe in ETH as the dominant smart contract network, it is not all blue skies ahead. ETH now faces extremely well capitalized competitors. While some boast strong

developer communities and rapid user growth, others have technological advantages, launching live on Mainnet with many or all of the features a fully upgraded ETH 2.0. Although many of these alternative L1s don't have differentiating features aside from lower fees (and less security), I would argue Ethereum is still in a race against time. As such, L2 protocols remain Ethereum's only hope to survive this competition, yet the outcome will result in Ethereum losing 99%+ of its potential fee revenue to L2 protocols. It will have to settle on taking the fees from said L2 protocols, which as previously discussed should be more than enough for it to survive if smart contracts become the main form of digital agreements society utilizes.

As technological progress is made, the cost of trust minimized computation will decrease over time. It is a deflationary resource which will asymptotically approach the cost of cloud compute, plus an additional cost for trust minimization which will vary depending upon the security of the chain. I believe ETH + L2s will offer the most secure computation per unit cost, and hence the most likely outcome is for Ethereum to become the DeFi chain. DeFi has the largest addressable market by an order of magnitude, with upwards of $700 trillion in assets capable of moving into the ecosystem over the next few decades. I believe its stature as the most secure L1 chain will cement it as the risk-free benchmark for the digital asset ecosystem. It is completely possible that other chains become winners for different applications, such as NFTs or gaming.

4 Chainlink

The first protocol enabling the creation of Decentralized Oracle Networks (DONs), Chainlink brings additional functionality to smart contracts. If Bitcoin is a calculator and Ethereum a computer, Chainlink is the internet. The internet provided computers with external connectivity, enabling advanced use cases such as E-Commerce, Social Media, Cloud Services, Video Streaming, and more. Similarly, before Chainlink the only actions that could be performed on Ethereum were creating new tokens, moving said tokens between wallets, and multi-key voting. Chainlink enabled the creation of DeFi, provably fair NFTs, decentralized insurance, algorithmic stablecoins, and more unique use cases.

Chainlink is not a blockchain, where every node in the network is performing an identical task to come to singular consensus. One can think of a DON like a build-your-own blockchain, but instead of validating blocks, each node in the network is validating some piece of data or computation *external* to the blockchain. It uses a variety of cryptographic protocols for DONs to come to consensus off-chain, before oracle reports are posted on-chain for smart contracts to consume. There are no specialized hardware requirements, therefore Chainlink uses approximately the same amount of electricity per node as a Proof of Stake system. Specifically, Chainlink is a heterogeneous network that supports the creation of any number of independent oracle networks. It was designed as a modular system from the ground up to support any potential use case for trust-minimized computation that blockchains can't performed due to their "walled garden" nature which is necessary for their security.

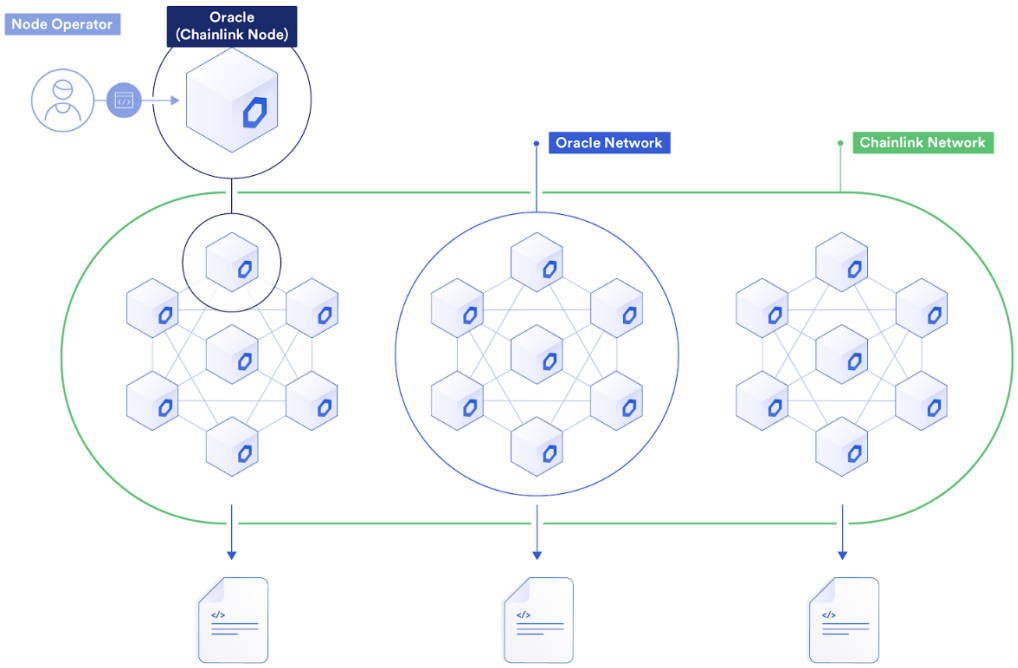

Figure 16 - Chainlink is a heterogenous network consisting of many distinct oracle network. Each oracle network consists of any number of sybil resistant nodes

The most common example is price data. There are over 800 Chainlink price feed DONs which come to decentralized consensus about the price of various assets that could be consumed by financial contracts. Navigating to https://data.chain.link/, we can observe one such price feed.

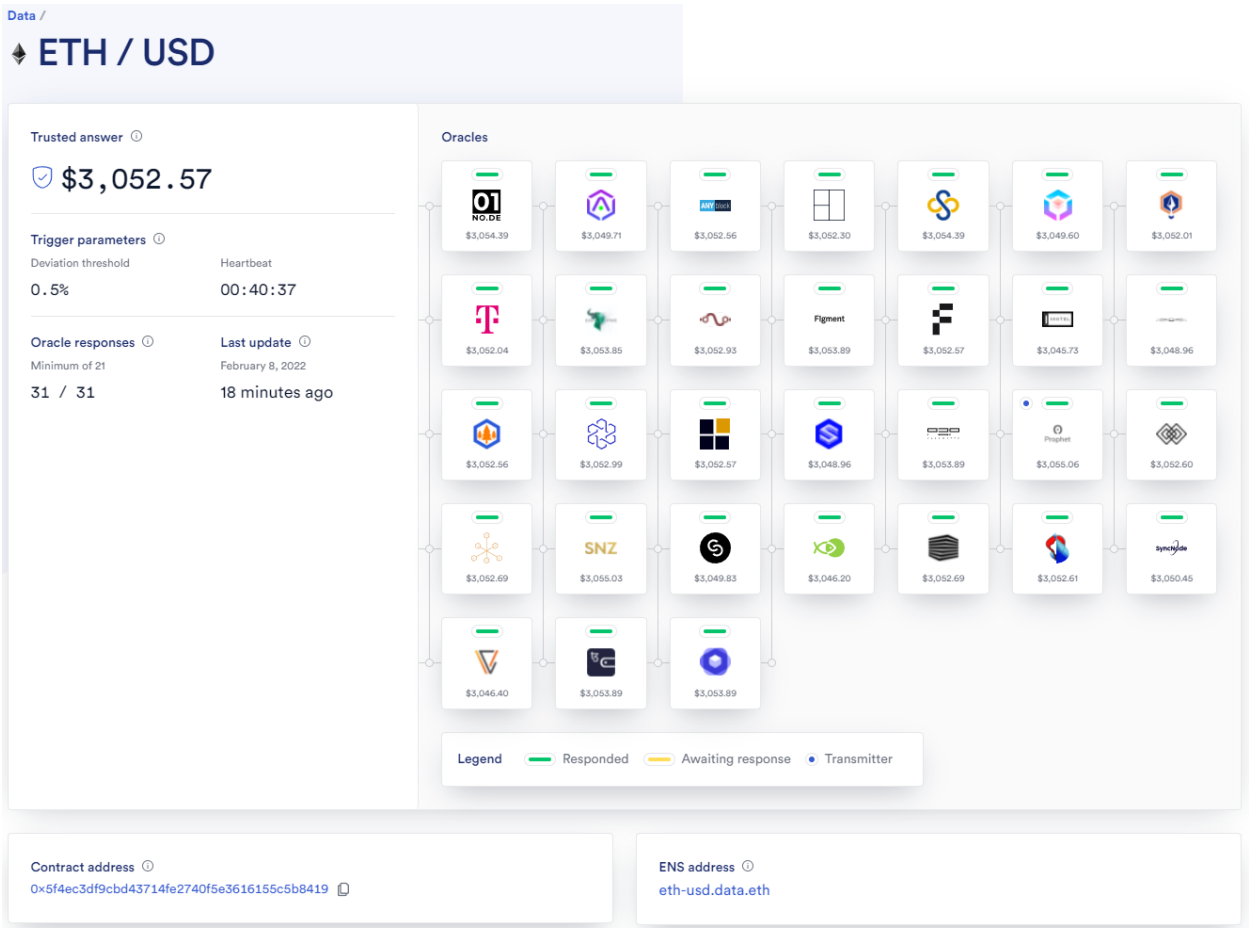

Figure 17 - Chainlink ETH/USD DON

Price feeds are just the tip of the iceberg – Chainlink oracle networks can perform off-chain computation as well. DONs can then relay the output of this trust-minimized computation to the smart contract that requires it. Some examples include Verifiable Randomness Generation (VRF), Proof of Reserves, Enterprise Abstraction Layer, Keepers (DONs that perform smart contract Dev Ops functions), and Cross Chain Interoperability.

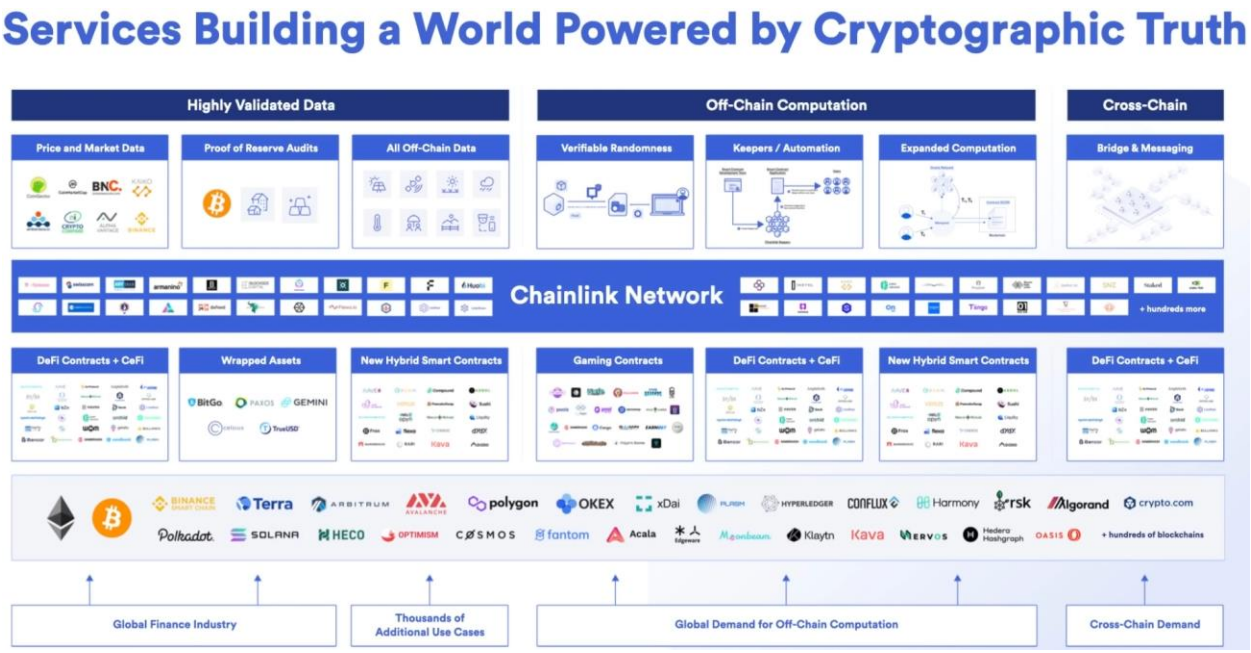

Figure 18 - Chainlink Network Services

The final, and most critical, point regarding Chainlink is that *nearly all smart contracts require off-chain data or computation*. Blockchains (such as Ethereum) provide the on-chain infrastructure, while oracle networks (such as Chainlink) provide the off-chain infrastructure. These technologies are synergistic, together enabling what are now known as hybrid smart contracts. As a result, Chainlink and a Layer 1 such as Ethereum share a large portion of their addressable market. In the following sections, I will compare Chainlink to Ethereum and other Layer 1s to analyze which protocol/s will capture the most value from this market. The two axes of comparison will be potential to earn yield, as well as the monetary policy of the token.

4.1 Future Fee Opportunity of the Chainlink Network

The first aspect of comparison between Chainlink and Ethereum/L1s is the potential cash-flow the network can generate. Note the total cashflow of a network is the summation of all fees paid to node operators. With respect to competition, Chainlink has a unique position as the largest oracle network provider, without a close second. Chainlink also offers many additional services which L1s do not.

4.1.1 Chainlink has Monopolized the Middleware Space

The first attribute that separates Chainlink from L1s is that Chainlink is a blockchain-agnostic oracle network. Chainlink is currently partnered with 90 L1s and is fully integrated and live on approximately 12 of said protocols.

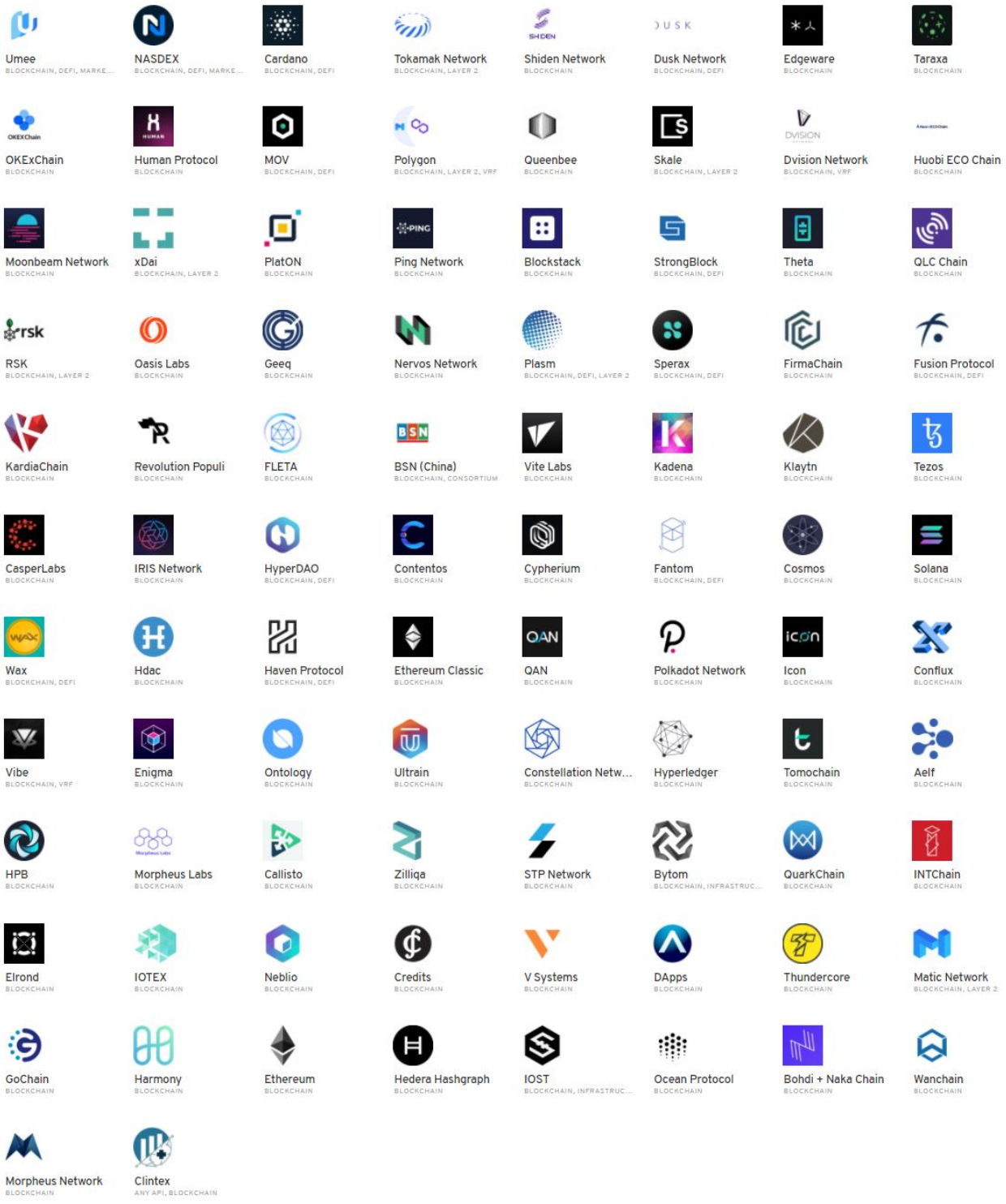

Figure 19 - Chainlink Layer 1 Partnerships & Integrations

Whereas Ethereum is competing with other L1s for market share, Chainlink has a monopoly on the oracle space. Navigating to defillama.com, we can see Chainlink Oracle's account for around 60% of TVS in the DeFi space.

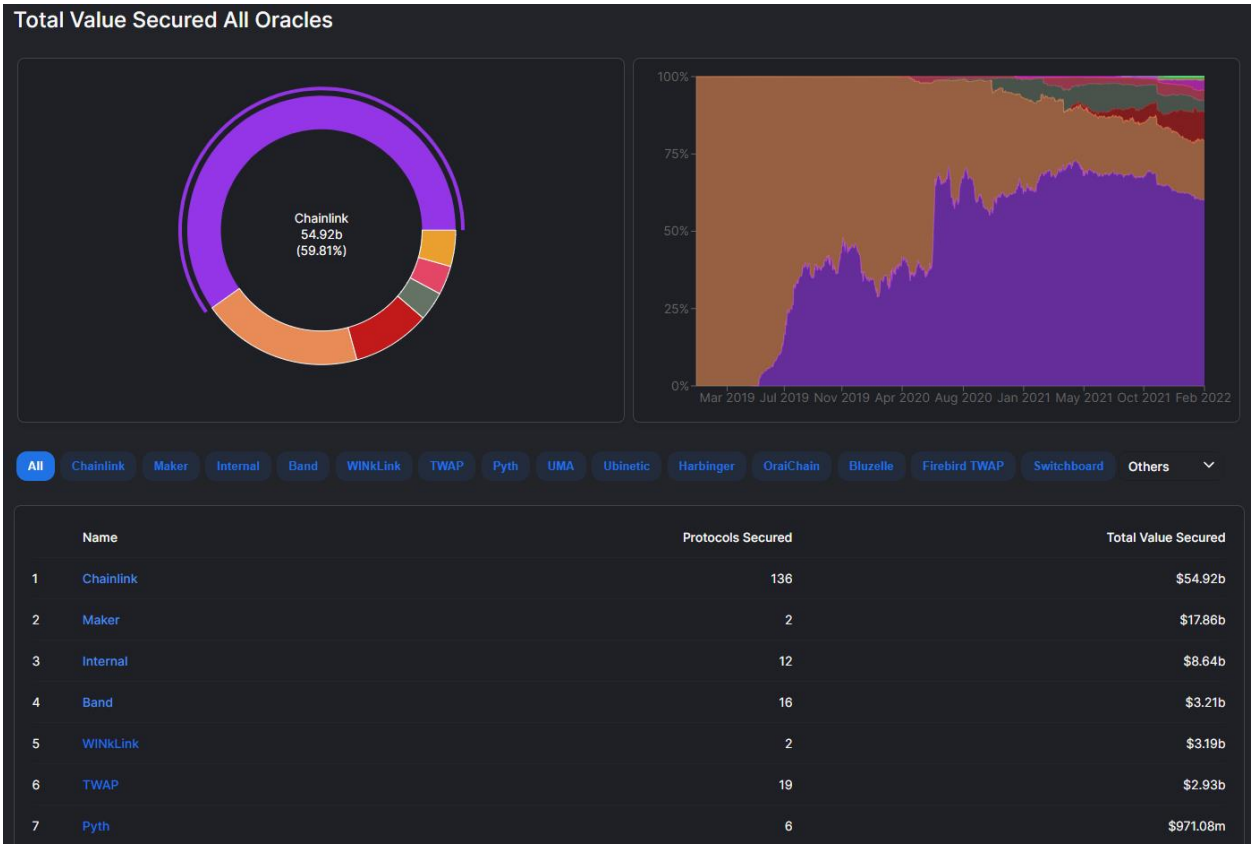

Figure 20 - Value Secured by various oracle networks

These numbers are misleading because some protocols use multiple oracle schemes. For instance, navigating to the second largest oracle network, Band, 4 out of the top 5 protocols that use it (ALPHA, DF, CREAM, and LRC) utilize Chainlink for their primary oracle. Note that these protocols account for 2.11 billion of its TVS. In reality, Band only secures around 1 billion in TVS, which is significantly less than Chainlink. The internal category refers to applications which utilize their own oracle scheme. Anchor protocol, which accounts for 8.45 out of the 8.64 billion in total TVS, just registered a failure of their Oracle Price Feeder, which accounted for over $37 million dollars in false liquidations [13]. Note that soon after, a governance proposal passed to switch their primary price feed oracle to a Chainlink price oracle [14]. This means the Internal oracle TVS is going to drops to approximately 20 million in TVS, and Chainlink's will grow by nearly 8.5 billion. In effect, Chainlink has 65 billion + in unique TVS, whereas Band Protocol (the 2nd largest oracle network protocol) has 1 billion in unique TVS.

Finally, Maker should fall into the Internal oracle category, but KEEP protocol uses their oracle so they are instead listed as an oracle network. Maker refuses to upgrade to Chainlink price oracles irrespective of several major oracle failures they have incurred in their past [15]. Regardless, Maker's oracle generally works with respect to their single use case, and they are not spending time innovating on their oracle design such that it can be used and trusted by other protocols. The overarching point here is that Chainlink does not have any true competition in the oracle space – their first mover advantage via founding smartcontract.com in 2013 has led to an insurmountable moat for competitors. Chainlink has over 350 employees with around 200 job openings, whereas BAND has around 25 employees. Every hybrid smart contract on every chain that hopes to secure significant value will need to use Chainlink, whereas ETH is

going to continue to fight for market share amongst competing public and private blockchains in different geographies and optimized for various use cases and transaction sizes.

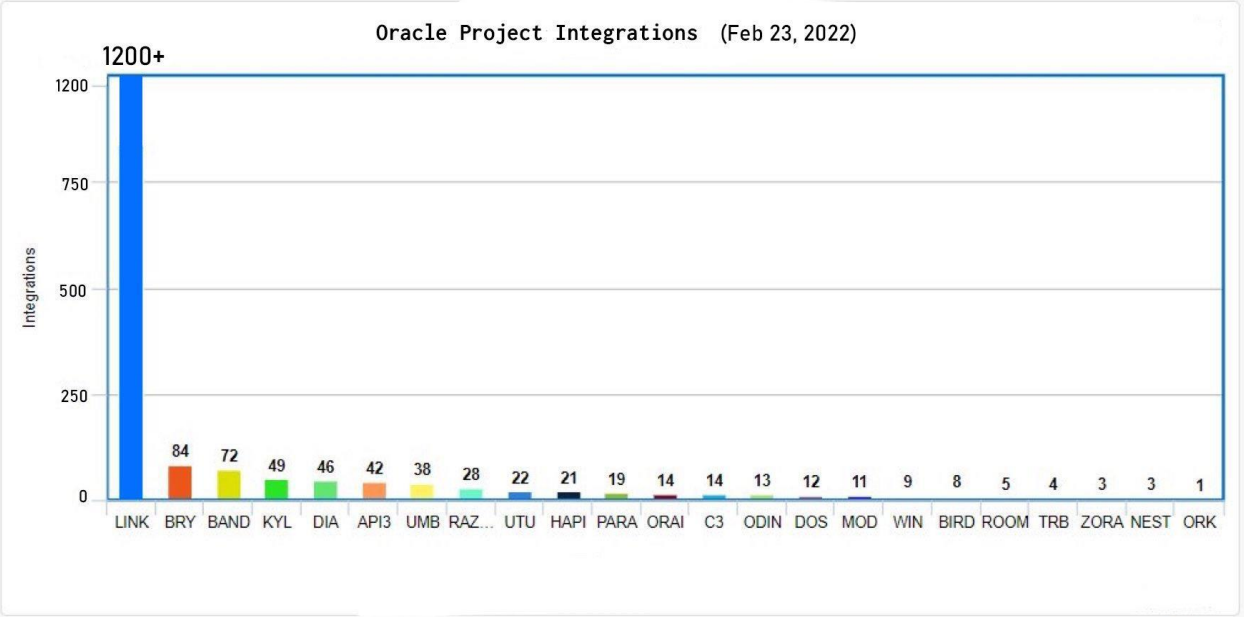

Figure 21 - Oracle Project Integrations

4.1.2 Chainlink Computation Services

Along with providing the necessary data for hybrid smart contracts to execute, Chainlink provides a host of additional services that L1s cannot perform.

4.1.2.1 Verifiable Randomness Function

Blockchains cannot generate randomness natively. Chainlink Verifiable Randomness Function v2 (VRF) provides provably random, tamper-proof, and low-cost randomness for smart contracts. Axie Infinity, the largest blockchain game by market cap, utilizes Chainlink VRF for many of the game functions. Blockchain gaming is going to be one of the largest use cases (and I believe the next hot use case) for smart contracts. Nearly every popular game today from Fortnite, Counterstrike, Call of Duty, World of Warcraft, etc. has in game marketplaces for in-game items. Many of these marketplaces rely on randomness to generate items for players. VRF is necessary to have provably fair item drops. At its peak, World of Warcraft had almost 20 million monthly active users. Not only do marketplace loot boxes require randomness, but in game item drops from monsters require randomness as well. One can easily imagine billions of monthly VRF calls, just for a single popular game.

With respect to collectable NFTs, the most popular and largest (by market cap) NFT project, the Bored Ape Yacht Club (BAYC) utilize Chainlink VRF for trait randomization and fair NFT drops of Mutant Serum NFTs. The vast majority of NFT drops will utilize VRF for randomness, whether that's profile-picture NFTs, or artists selling generative art.

In 2021 Chainlink VRF calls went exponential and ended the year with over 2.5 million calls, and with 285 projects integrating VRF. I believe 2022 is going to be the beginning of blockchain gaming, inspired by the success of Axie Infinity. I can easily see this number 10x by years end.

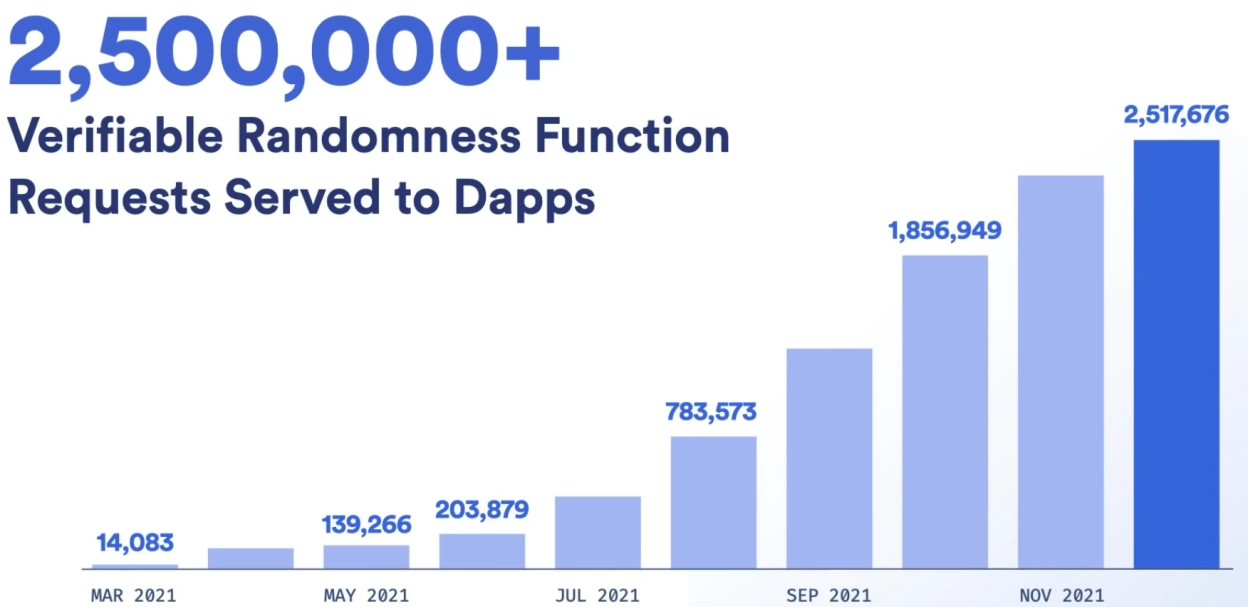

Figure 22 - Growth of VRF calls

4.1.2.2 Keepers

Smart contracts alone can't trigger or initiate their own functions at arbitrary times or under arbitrary conditions. State change will only occur when a transaction is initiated by another account (such as user, oracle, or contract). To resolve this issue, Chainlink developed the Keepers network: A decentralized network of nodes that are incentivized to perform all registered jobs.

Chainlink Keepers can be leveraged to perform a variety of DevOps services and off-chain computations on behalf of hybrid smart contracts, including to:

- Execute limit orders on decentralized exchanges
- Mint tokens when reserves increase
- Harvest yield from vaults
- Rebase elastic supply tokens
- Rebalance on-chain trading and yield farming strategies
- Liquidate undercollateralized loans
- Release locked assets after periods of inactivity
- Top up token balances falling below a minimum threshold
- And many more possibilities yet to be discovered

As one can see, the vast majority of DeFi protocols can utilize Keepers in some way. Limit orders alone is a massive use case that every DEX will need to integrate if they ever hope to compete with centralized exchanges. If DeFi becomes the global financial infrastructure, Keepers will play a crucial role in fully automating, and decentralizing, the many services that are required.

4.1.2.3 Proof of Reserves

Chainlink Proof of Reserves provides definite on-chain proof of any asset's true collateralization. By providing automated audits from a decentralized network of oracles, a financial service can improve

transparency for users and prevent systemic failures from insolvency. Proof of reserves works for both on chain and off chain assets.

Wrapped Bitcoin (wBTC) is the first and only way users can bridge BTC onto the Ethereum blockchain to use it as collateral in DeFi products. BitGo, the exchange that offers this service, utilizes Chainlink proof of reserves to boost the transparency and auditability of wBTC. The circulating supply of wBTC is over 260,000, currently $10.4 billion.

One can imagine a future where instead of audits taking place once per year by companies who are buddy-buddy with the banks, audits taking place every 1 minute by an unbiased, transparent, decentralized set of nodes. This is a future that could limit crises like the 2008 Great Financial Crisis. As DeFi grows in popularity, users will demand full transparency behind the services they utilize. Proof of Reserves offers a way for centralized (CeDeFi) companies utilizing DeFi infrastructure to provide the same assurances as DeFi protocols. As I believe there is a place for CeDeFi companies (many users enjoy interacting with a company with customer service, as well as don't trust themselves to manage private keys/funds), Proof of Reserves is a crucial tool that will enable these companies to compete in this new landscape.

4.1.3 Chainlink as a Layer 0: CCIP and the Enterprise Abstraction Layer

4.1.3.1 Cross Chain Interoperability Protocol

As I discussed earlier, Chainlink is much more than a data delivery network. A committee of Chainlink nodes forming a DON can come to consensus on any set of data or computation. One application of this is utilizing Chainlink for interoperability between any two enterprise systems or blockchains.

Chainlink is currently developing the Cross Chain Interoperability Protocol (CCIP) with plans to release it this year (2022). CCIP aims to establish a universal connection between hundreds of blockchain networks, both public and private, by creating an open-source standard for cross-chain communication. CCIP provides smart contract developers with a generalized, compute-enabled infrastructure for transferring data and commands across blockchain networks. This will allow for cross-chain smart contracts which utilize the strengths of various blockchains simultaneously. Users will no longer need to bridge tokens between chains to utilize different services. CCIP allows dApps to abstract away the complexities of transferring tokens to different chains, and instead allow users to directly interact seamlessly with many chains simultaneously through a single frontend. Users won't even know what blockchain they are operating on.

One can imagine a future where every decentralized application offers cross-chain smart contracts. If a cross-chain lending protocol connects to every single chain and provides users with the most liquidity and cheapest rates for loans, it would be hard for a single-chain lending protocol to compete. A cross-chain yield protocol can deposit users' capital to any DeFi application across any chain to always provide the highest yield.

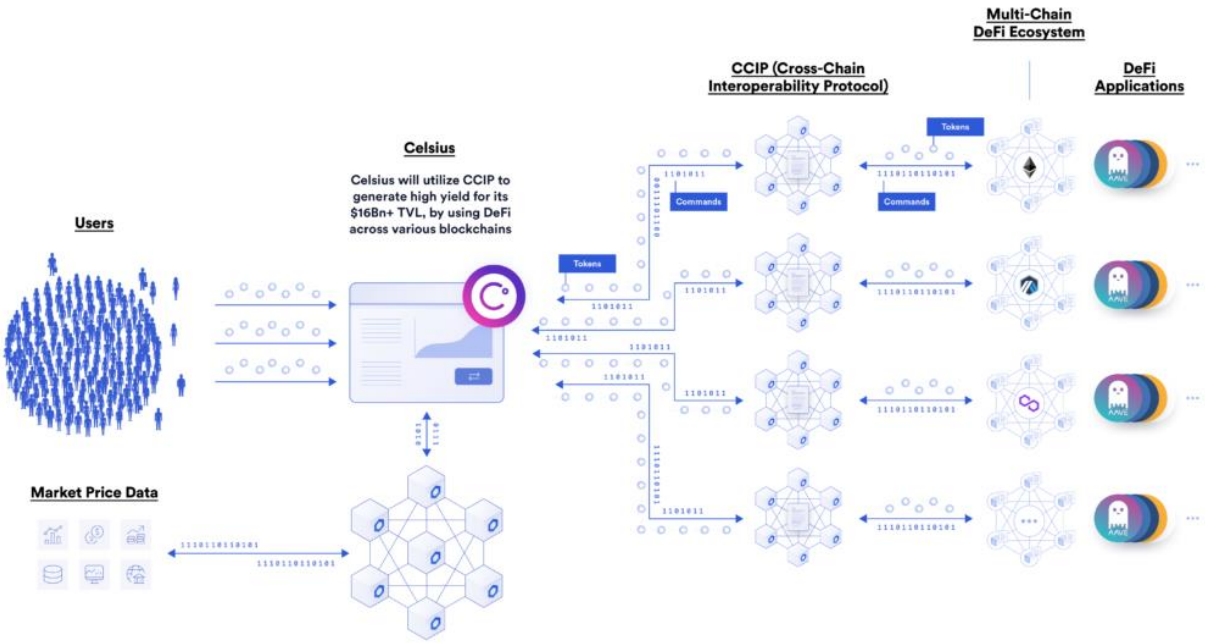

Figure 23 - Example of cross-chain yield farming

A similar dynamic with exist with DEXs, where the cheapest trade is always found and executed via CCIP. Any time any of these events occur, LINK will need to be paid to the node operators processing this cross-chain interaction.

4.1.3.2 The Enterprise Abstraction Layer

Centralized enterprises are beginning to realize that interacting with smart contracts and blockchains is the future. Interacting with services such as DeFi and NFTs represent new revenue streams, and possibly the only way for legacy companies to retain their users. Let's take a look at banks as a primary use case.

Nobody is going to store their money in a bank which offers a 0% interest account, when one can get 8% relatively risk-free with DeFi solutions. If inflation persists and remains high, this will only accelerate the adoption of DeFi. If banks what to utilize DeFi to get access to these yields, they run into some fundamental problems. For one, what blockchain do they build out infrastructure for? There are over 100 blockchains and many more on the way. It is impossible for anyone to predict which blockchains will remain popular. A bank would have to constantly hire new teams to create the infrastructure to interact with dozens of blockchains they wish to conduct economic activity on. This is where Chainlink comes into play. Chainlink can be used as a blockchain abstraction layer to securely connect any existing system or API to any private or public blockchain through a single adapter.

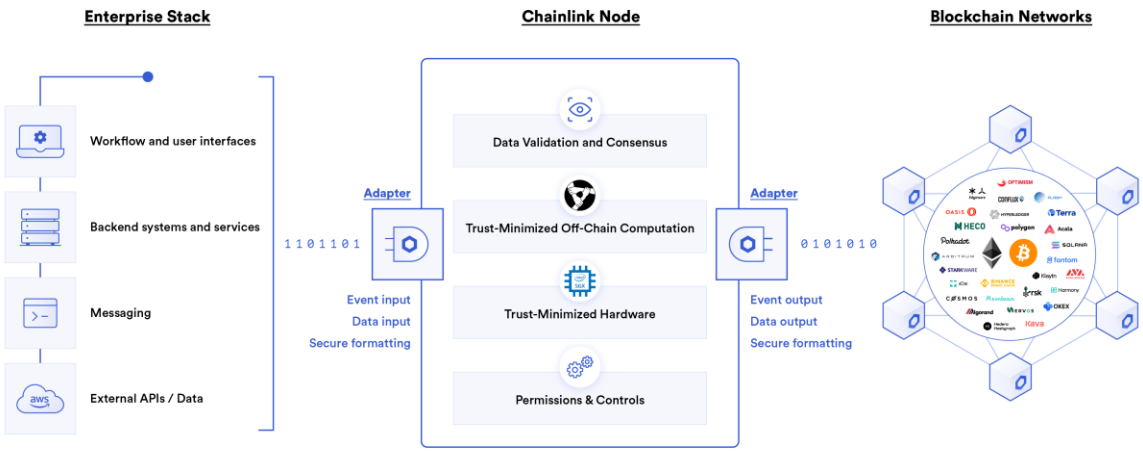

Figure 24 - The Enterprise Abstraction Layer

Chainlink is the only enterprise-grade oracle network that enables organizations to do this, supported by Chainlink's growing network of node operators. This is why the World Economic Forum has collaborated with Chainlink to create a blockchain middleware standard [17]. Chainlink has also partnered with SWIFT. Utilizing SWIFTs Public Key Infrastructure (PKI) which is already connected to over 11,000 banks and 2 billion end users as the global standard for inter-bank messaging, almost every bank in the world can interact with smart contracts without having to change their backend infrastructure or retrain any employees on how to use said software [18]. Now any bank can interact with any smart contract on any blockchain via the Chainlink abstraction layer and CCIP.

4.2 Protocol Revenue Analysis

Over time, the Chainlink Network's revenue will increase as more and more of its services are adopted.

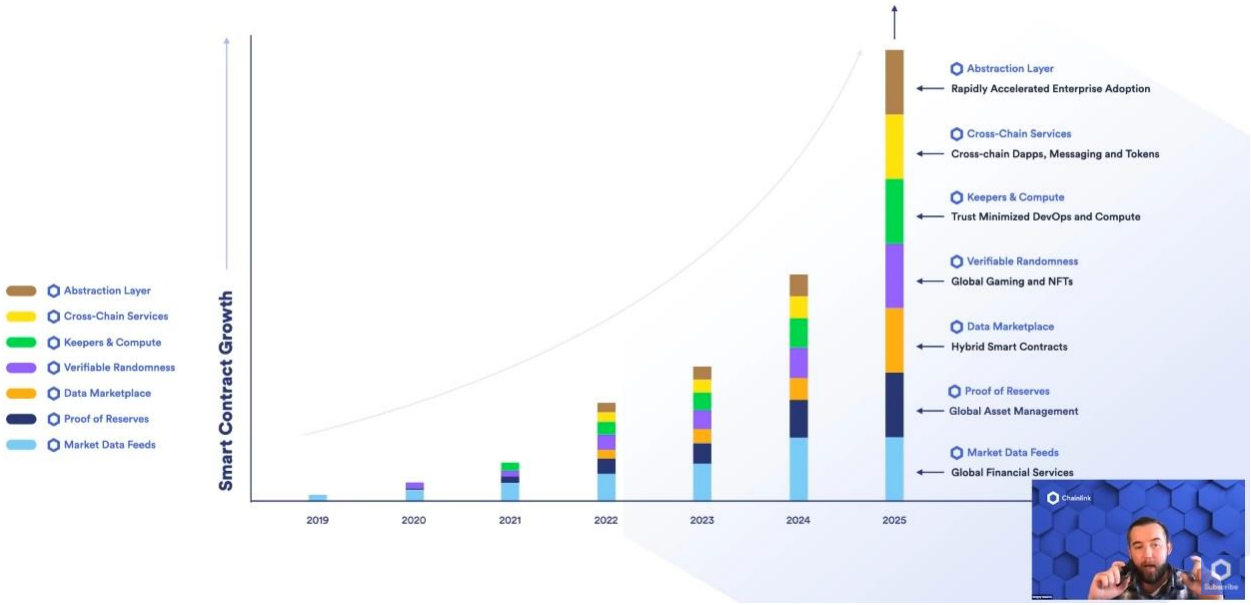

Figure 25 - The Chainlink Network's Revenue Generating Services

4.2.1 Data is a Minimally Deflationary Resource

Comparing the fees captured in the last 90 days between layer 1 protocols, ETH is dominant, and it is not particularly close.

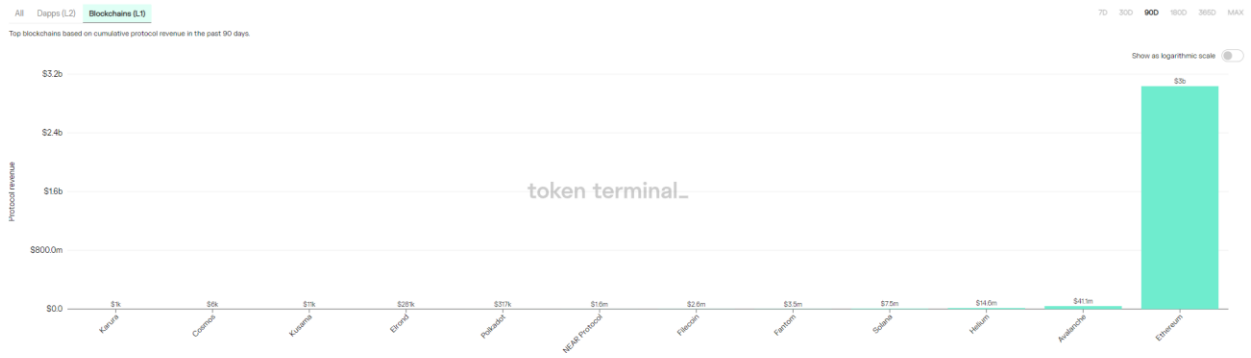

Figure 26 - L1 protocol fee revenue

This chart is misleading, though, because Ethereum fees are sky-high. Since inception, there have been approximately 1.478 billion Ethereum transactions, with an average fee of $18.53, in total generating $27.40 billion in protocol revenue. When comparing this to an L1 protocol at the other extreme of fees, Solana, we see how fee size can distort protocol revenue. Solana fees are a fixed $0.00025. Since inception, Solana has performed just over 59 billion transactions. With the fixed fee cost listed above, Solana has generated around $14.75 million in protocol revenue, three orders of magnitude less than Ethereum. Although Solana has existed for a few years less, this discrepancy would barely change if one normalized length of time from launch.

This is why using current numbers for fee estimates is a waste of time. Currently, a fully optimized rollup is capable of $0.10 transactions with 4,500 TPS [20]. Over time, layer 2 scalability solutions when combined with a fully upgraded/sharded Eth 2.0, will result in sub-Solana fees, and a throughput of potentially 10 million transactions per second. As this continues to progress and users fully migrate to L2 (note that this migration could happen without users knowing it via the Chainlink CCIP abstraction layer), the only demand for ETH will be coming from layer 2 solutions, as retail ETH demand will have switched to layer 2 token demand to interact on rollups.

As I discussed in Section 3.3, trust-minimized computation being deflationary results in an inverse relationship between user adoption and fees. Not to mention, the vast majority of these fees are going to go to the rollups, not Ethereum. This is why Chainlink has a distinct advantage with respect to future fee opportunity.

Chainlink inherently provides different services than Layer 1 protocols. The primary service that sets Chainlink apart is that it is a network to deliver real-world data to smart contracts. Although I would argue data is a deflationary resource, I would argue it is less deflationary than on-chain trust-minimized computation.

Let's look at price data, for example. Asset prices, such as the price of Apple stock, Oil, or Bitcoin, is generated on exchanges as traders buy and sell the asset. Exchanges like the NYSE, Nasdaq, or Coinbase sell this data directly to Chainlink node operators, or to data aggregators who then sell it to Chainlink node operators. Irrespective of how many oracle networks exist, there are only a finite number of exchanges who produce this data. In order for the price of this data to come down, there must be new exchanges who dilute the market. Although it is theoretically easy to create an exchange, it is incredibly hard to create an exchange which is actually used. Exchanges have network effects because traders seek out liquidity to get the lowest slippage with trades. To compete with established exchanges, new exchanges must accumulate substantial liquidity. This is incredibly difficult to do, as established exchanges network effect and moat only increase over time, making it increasingly hard to disrupt them. This is why price data is inherently stable, or slightly deflationary.

For something like weather data (which could be utilized to trigger insurance contracts), the data is typically generated through satellite imagery. Although the cost to launch a satellite has decreased significantly with the rise of private rocket companies like SpaceX, it is still extremely expensive. As such, although I do expect the cost of weather data to decrease slowly over time, this will be a slow trend as re-usable rocket technology continues to advance, and on-ground sensor networks are built out.

The per-unit cost of a price-feed supplying price or weather data is going to remain pretty stable in the short and medium term. It is priced in USD, but smart contract operators must pay in LINK tokens. Navigating to Market.Link, we can see over the past 90 days Chainlink node operators have been paid around 2.2 million LINK tokens. With an average price of approximately $21.05 in the last 90 days, this equates to around $50.19 million in protocol revenue delivered to node operators. This would put LINK at 2nd in terms of previous 90 days protocol revenue. Still a distant 2nd to Ethereum, but greater than Avalanche and Solana in terms of revenue.

The key takeaway here is that as Ethereum fees are going to decrease over time, LINK fees will not decrease as much on a relative basis, for data delivery services. As the number of users, dApps, and

transactions increase on blockchains over time, LINK fees will continue to increase proportionally, whereas ETH will decrease exponentially as rollup technology progresses.

4.2.1 Interoperability Appears to be a Winner-Take-All Market

I am yet to mention fees generated by Chainlink as an Abstraction Layer, as well as fees generated by CCIP. Chainlink is going to monopolize the Enterprise Abstraction Layer market because of their first mover advantage and partnership with SWIFT. As previously discussed, instead of having to build out the PKI infrastructure which is already fully integrated into over 11,000 banks in the world, Chainlink is leveraging SWIFT's system. Banks do not need to upgrade any of their legacy infrastructure or retrain any of their employees to utilize said infrastructure. Any competing network would need to build out this entire infrastructure on their own. As SWIFT has had a monopoly on inter-bank messaging for nearly 50 years, I find it hard to believe that this market is easily disrupted. Although I believe the SWIFT system itself will eventually be disrupted by blockchain-technology & cryptocurrency, it's software infrastructure will be vital for 10s of thousands of companies to interact with the new blockchain-based financial system.

The World Economic Forum argues the benefits of all users choosing a singular, open-source interoperability framework in reference [17]: This produces the lowest cost for end users, a singular set of documentation where contributions benefit the entire network, and ensuring that no single party gains an unfair advantage from owning the IP or sole development rights. Naturally, the open-source middleware which generates the largest network effect will necessarily become the only solution utilized. I believe it is a foregone conclusion that the Chainlink network will become the global standard for Enterprise-Blockchain interoperability. Any time a bank or enterprise sends a command to a smart contract, they will need to pay LINK to the Chainlink network. As I believe it is highly likely that smart contract-based infrastructure replaces almost all existing legacy financial, insurance, and trade finance-based infrastructure, the revenue from this market is significant.

Similarly, if Chainlink CCIP becomes the global standard for Blockchain-Blockchain (or cross-chain) interoperability, this produces potentially the largest revenue generating opportunity for the Chainlink network. There are dozens of teams attempting to solve cross-chain interoperability, but none that are as uniquely placed to succeed as the Chainlink Network.

Chainlink is already integrated and trusted by over 1200 protocols for price feeds and other data. Chainlink is currently securing over $60 billion in TVS across 12 different protocols and has the largest amount of value to be used as collateral for bridging solutions. Any protocol which utilizes Chainlink for price feeds will likely also use CCIP for cross-chain smart contracts. Aave, the largest lending dApp by TVL, has already committed to using CCIP for Aave v3. Celsius, one of the largest CeDeFi yield aggregators with over $26 billion in TVL, has committed to using CCIP as well. With these two applications alone, Chainlink CCIP powered TVL dApps would have the 2nd highest TVL among all layer 1 protocols. Due to Chainlink's large userbase, I fully expect many more to announce the use of CCIP once it is released.

Second, Chainlink CCIP will exist as a base-layer messaging protocol, allowing it to send commands as well as tokens between chains. Although there are multiple bridging solutions live, none have the ability to send commands. As opposed to users having to manually send tokens with a bridge, users will be able to interact with dApp front ends and have all cross-chain processes abstracted away from them. Due to this dynamic, I believe CCIP will become adopted much faster than isolated bridges which require their own application.

Looking at some of the highest bridges by TVL, we have RenVM, Thorchain, Wormhole, and Hop Protocol with $1.16 bil, $0.150 bil, >$1.0 billion, and $0.122 billion respectively. None of these protocols secure even close to the amount of value Chainlink secures, and it must be noted that we have already seen a massive bridge hack. Recently, in the 2nd largest DeFi hack ever, Wormhole was hacked for 120,000 Ether – around $320 million at the time [19]. Security is Chainlink's specialty, and the network is yet to be hacked or fail in its entire history. Chainlink CCIP is the application of Chainlink's highly secure consensus mechanism (OCR 2.0 that currently secures more than $60 billion and has done that successfully for multiple years) to the problem of cross-chain communications. As such, the security they currently provide for other systems is fungible to a degree with cross-chain interoperability, because it uses the same consensus mechanism.

With a team of over 350 employees which is likely set to double by years end (based upon job opening numbers), they have over an order of magnitude (or two) more employees than any other bridging protocol, and likely more employees than every other bridging protocol combined. The inventor of pairing based cryptography, Dan Boneh, recently joined the team to help work on CCIP. Their team is un-rivaled – both with respect to talent, size, and runway. Once CCIP is released, the amount of TVL within CCIP smart contracts will grow to around $40 billion in TVL, 40x greater than any competing bridge solution. Because of Chainlink's relationships with over 1200 protocols they are already partnered with, the pathway to further extend its TVL lead already exists.

With respect to bridge operation, Chainlink already has the infrastructure in place. The network has 337 distinct, high-performance node operators. These node operators have a long history of on-chain performance and can begin providing CCIP services at launch. The second CCIP goes live, Chainlink will have the capability to create the most decentralized bridge, with the strongest trust assumptions. The Chainlink staking mechanism can also be utilized to further increase the security of said bridges.

Because of the advantages discussed above, I believe Chainlink CCIP will become the standard for all Blockchain-Blockchain interactions. This means any time a cross-chain smart contract is called, a payment of LINK must be made to the node operators that send the CCIP commands to every chain called within the contract. Whether this contract sits on Ethereum, Solana, Arbitrum, or Avalanche, LINK will need to be paid to the node operators for CCIP functionality. I believe cross-chain smart contacts will become the standard for the vast majority of blockchain use cases and generate significant revenue for the Chainlink Network.

4.2.3 Userbase for L1s vs. LINK & Expected Transaction Volume

L1s and Chainlink inherently have a different userbase. The main distinction here is that end-users need to purchase the base layer token to interact with any application. End users do not need to purchase LINK to interact with a dApp. Instead, it is the dApp that must purchase LINK to pay for data feeds, VRF, Keepers, Proof of Reserves, or CCIP bridging. As a result, currently there is much more demand for base layer tokens than there is for LINK. We have also seen NFTs explode in popularity. Many NFT projects do utilize Chainlink, but once again it is the project itself which must purchase LINK for VRF requests, or to generate floor price feeds such that NFTs can be used as collateral in lending protocols. Base layer tokens benefit more from NFT trading volume. This is because users must purchase ETH to buy and sell NFTs on marketplaces like OpenSea. It is easy to see that the userbase for LINK is much smaller than the userbase for L1 tokens.

As a result, it is not surprising that up unto this point L1 protocols have sustained higher market caps than Chainlink. A simple framework to value protocols is by looking at the Metcalf's law valuation – effectively predicting price based upon the number of wallet holders. The number of wallets on Bitcoin, Ethereum, and Chainlink has supported this claim.

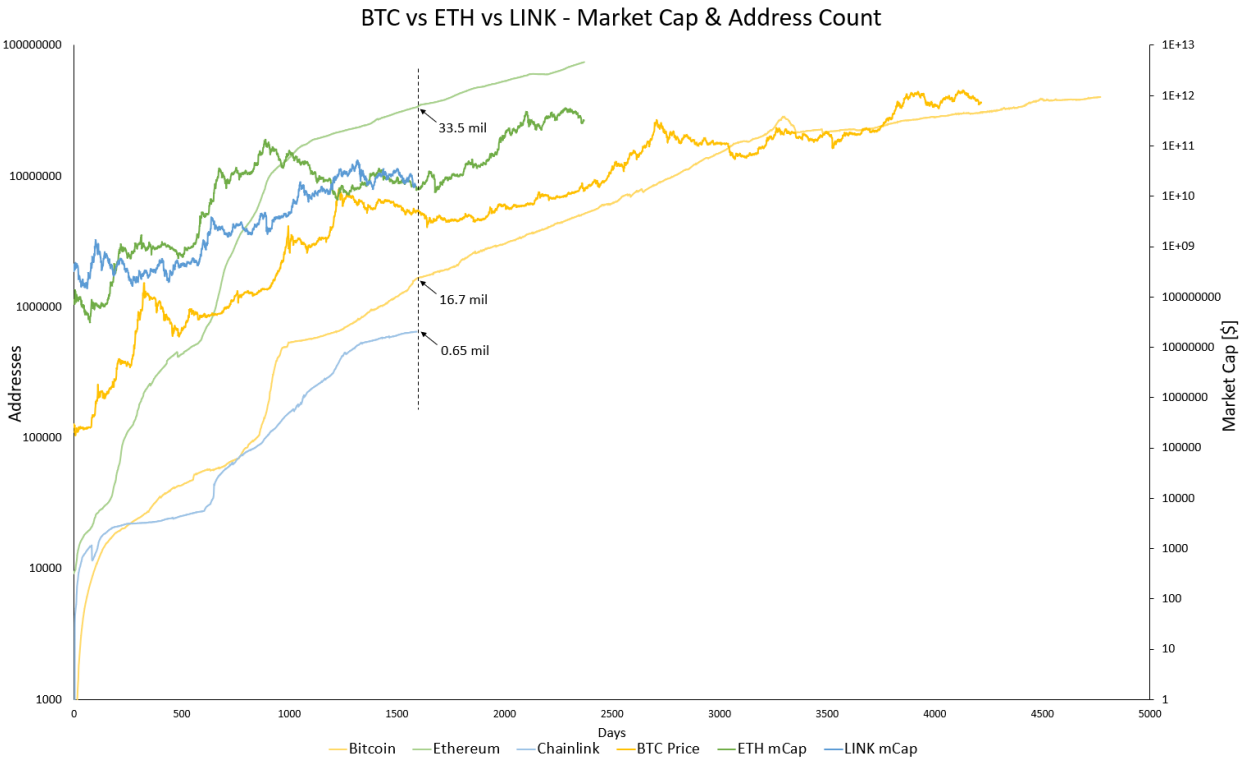

Figure 27 - LINK vs BTC vs ETH Market Cap and Addresses from time of inception

What is most interesting to note, though, is that at this point in each protocol's lifecycle, Chainlink has the highest market cap, albeit slightly. Chainlink and Ethereum, roughly 1250 days post ICO, have roughly equal market caps, yet Chainlink has approximately 2% of the number of wallet holders. This deviation should not go unnoticed, as Chainlink has been able to reach a high market cap in a short period of time, with inarguably less retail overall demand than BTC or ETH.

I believe the main reason for this deviation is the differentiation between LINK and ETHs userbase. Number of wallets is a poor metric because in the case of Chainlink, its userbase are dApps. These smart contracts are singular addresses which interact with the LINK contract constantly 24/7 as they consume oracle reports. Unfortunately, on-chain metrics websites do not capture this data, and the Market.Link API is still in its infancy (although I have contacted the team and they have stated they have a large upgrade planned so that users can view the entire history of any relevant LINK network data). In a recent post by Chainlink, though, they announced that they have posted over 1.1 billion data points on chain as of January 1, 2022.

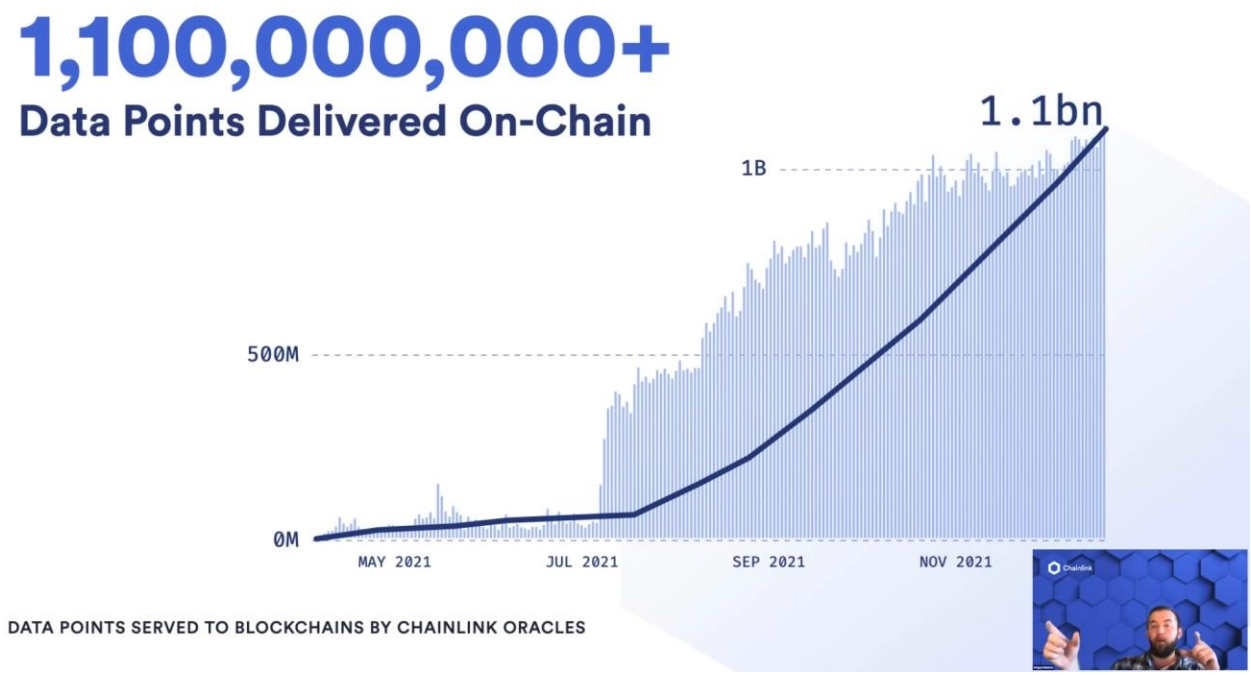

Figure 28 - On-chain data delivery by Chainlink Network accelerated once live on high-throughput blockchains

The Chainlink network can post data or computations on-chain at the speed of the underlying blockchain it is integrated into. Note the massive increase in on-chain data points delivered around July 2021 – this was a few months after Chainlink went live on higher throughput blockchains such as BSC and Avalanche. When Chainlink was only live on Ethereum, due to the slow nature and high gas costs to post data points on chain, dApps used a shared fee model where a singular Chainlink price feed was paid for by every dApp that consumed it. These price feeds update prices around every hour or so, or if the price moves based a specific deviation threshold, typically 0.5%. In a sense, the Chainlink price feeds became public goods for the DeFi ecosystem. With every new user the cost/user dropped, while the network generated more fees for node operators and became more secure.

On higher throughput blockchains with sub-second latency times and low costs, this has opened the door for dApps to create their own oracle networks that post oracle reports *any time* a transaction occurs. This creates the most accurate price feeds, which for applications such as DEXs creates the lowest risk environments for potential false liquidations. What does this mean for the Chainlink network? I believe as all user activity moves to higher throughput blockchains, more and more custom oracle networks are going to be created which will result in substantially more transaction calls to the Chainlink network. Although the number of transactions on the Chainlink network pales in comparison to L1 chains, I believe it will catchup over time due to this dynamic. In particular, I believe VRF and CCIP are going to go exponential in transaction calls over the next few years. Any time any user uses a DeFi dApp, it will make a CCIP call as that contract scans every chain to see where transaction will be cheapest/yield will be the most/etc.

Chainlink network calls will never be as great as total L1 transactions, but it is possible the network generates more transactions than any *single* blockchain. When one takes into account the size of these transactions (versus deflationary L1 transactions), I expect the net fees for the Chainlink protocol to be

greater than any single blockchain as well. The Chainlink network will also generate transactional throughput by acting as an enterprise abstraction layer – something that cannot be underestimated as the 4th Industrial Revolution unfolds, and we move into an autonomous economy driven by IoT, AI, and Hybrid Smart Contracts.

4.3 Chainlink Staking: The Apex of Cryptoeconomic Design

4.3.1 LINK vs. ETH Staking: Non-Diminishing Staking Yields

When the monetary policy of two tokens is compared, typically we are looking at how the token is distributed between token holders, how it is utilized to encourage specific behaviors, and finally how the token itself responds to said behaviors. These aspects culminate in the token supply being deflationary, stable, or inflationary over various time horizons. Ultimately, a scarce token is beneficial to token holders for obvious reasons.

Scarcity does not necessitate value, although under the right circumstances they can be correlated. For instance, aside from 2021, Apple's earnings have been flat since 2015, but because of their record number of stock buybacks, their earnings per share have increased substantially. This can be thought of as financial engineering to make the stock "appear" more valuable. The total dividends returned to shareholders remains the same, although on a per share basis it has increased. Here I would argue scarcity is not indicating Apple as a more valuable company.

Looking at Ethereum's cryptoenomics once EIP-1559 was released, one can see by burning base transaction fees and reducing the supply of ETH, a similar "financial engineering dynamic" is taking place. For the purpose of this thought experiment, assume that every validator of Ethereum does not purchase or sell any Ethereum. Effectively, the entire supply would be locked up by the validators. As I detailed in Endnote (i), the relative ownership of every validator in the network would remain equal. If base fees *were not* burned, then every validator would have extra ETH emissions to either re-stake or convert to other assets. Because every validator would not re-stake all ETH, some of the earned fees would not be reinvested in the network. By forcing base fees to be burned via EIP-1559, it simulates the effect of all validators being "forced" to re-stake all earned ETH from transaction fees. The analogy here would be a company having a mandate to use a fixed % of all revenue on stock buybacks.

Although I believe EIP-1559 does produce long-term value for the network and is beyond financial engineering (because it aligns all network participants to return value to the network), at the end of the day Ethereum retains the problem of not having enough base fees to completely pay validators. They rely on the Proof of Stake rewards approximately 60-70% to secure the network, and as a way to create a non-volatile reward mechanism. This is crucial because at all times the network must incentivize enough users to stake – in times of low usage where fees could drop substantially the network still needs validators to ensure it is secure. This is where I see the first weakness of Ethereum's staking mechanism as compared to Chainlink.

There are diminishing returns to EIP-1559 fee burning. As more and more individuals stake their ETH, to keep yields relatively desirable (such that users are incentivized to stake), the protocol must "print" more and more ETH. Navigating to Figure 7, one can see that once the vast majority of supply is locked (approximately greater than 83.5%), the APY drops to 1.81%, and the inflation rate increases to 1.71%. As the inflation rate increases, if it becomes greater than the amount of fees that are burned, the protocol will once again become inflationary. Over time as fees come down and move to L2 protocols, if the

increase in usage does not offset the decrease in costs there will necessarily be fewer base fees that are burned. This could also contribute to not enough ETH being burned to keep it deflationary. The lower APY in tandem with a potentially less deflationary, or inflationary ETH, could incentivize validators to un-stake their ETH and instead provide liquidity elsewhere.

I want to emphasize that this is not necessarily bearish for Ethereum. If more than 83.5% of the supply is staked, that is on its own incredibly bullish because the free float supply has been reduced massively. What this does indicate, though, is that there appears to be an upper bound on the benefits of EIP-1559. A virtuous cycle exists where, initially, users are incentivized to stake ETH and receive high APYs. But after a certain point where the vast majority of ETH is staked, a vicious cycle will begin as validators un-stake ETH to search for better yields or assets with stronger store of value properties. I believe there is some equilibria point in the middle, which as I discussed is APYs somewhere around 5% and a stable or slightly deflationary ETH. As smart contract technology is adopted over the next 10 years, ETH should continue to appreciate like a market leading FAANG tech stock. Although it won't return 10-20x multiples into perpetuity, I expect its performance to beat the S&P and NASDAQ for the next decade. As likely the foundational L1 network for DeFi, it is also important to note that this yield will likely be viewed as the risk-free benchmark for the fixed income space. As such, I believe Ethereum will offer top-2 risk-adjusted yields in the space. Many investors would choose a stable 4-5% from Ethereum (where they know the underlying asset will retain/go up in value) as opposed to an 8-10% for a more volatile PoS asset.

Shifting to Chainlink, the first reason why it has a stronger staking mechanism is because staking rewards *do not* experience diminishing returns. Chainlink operates with a highly efficient off-chain consensus mechanism (OCR 2.0), leading to many Chainlink DONs being completely self-sustaining from user-fees alone – no "block-reward" is necessary. Although the team had to utilize 117 million LINK tokens out of the 350 million LINK incentivization fund as a "block reward" to incentivize early oracle networks, the team has frozen this fund since November 19, 2021. With no block reward diluting the supply, this allows node operators to capture all network fees, which are denominated in USD, but paid in LINK.

The implication of this is that *Chainlink node operator APYs will not decrease as more entities stake their tokens*. Whereas the ETH staking APY decays to sub 2% as 80+% of the supply is staked, the Chainlink APY will remain at a fixed %. Because the Chainlink network will likely have a higher cashflow than any L1 network, the top node operators will experience higher USD denominated APYs as well. This means there is no vicious cycle that will reduce LINK staking APY as more entities stake, encouraging all entities to keep their tokens staked. This has a secondary effect which effects the monetary premium of LINK – it will lead to a massive reduction in the free float supply.

4.3.2 Staking will Drastically Reduce the Free Float Supply

Staking in Chainlink is inherently different than staking in Proof of Stake blockchains. When two parties create a smart contract that requires external data, they will then create a decentralized oracle network of node operators to provide the data or computation for that contract. Using reputation scores, collateral requirements, and the Chainlink Marketplace, the parties can hand select the individual nodes that they want providing this data. It is at this point that the nodes and contract creators will come to terms on a binding Service Level Agreement (SLA), where the terms for delivery data, as well as payment if done correctly, are outlined. This is where staking comes into play. In the terms of the SLA, the contract creators can require the node operators to post collateral against their terms of the job. The amount of collateral posted is dependent on the number of nodes in the network and the total amount of value up for transfer

in the hybrid smart contract. Collateral will likely be valued in USD terms but must be posted in LINK tokens.

The implications of this cannot be understated: *The amount of collateral posted for contracts must scale with the size of the contract.* The World Economic Forum estimates $866.9 trillion could eventually move into DeFi over the next few decades [23].

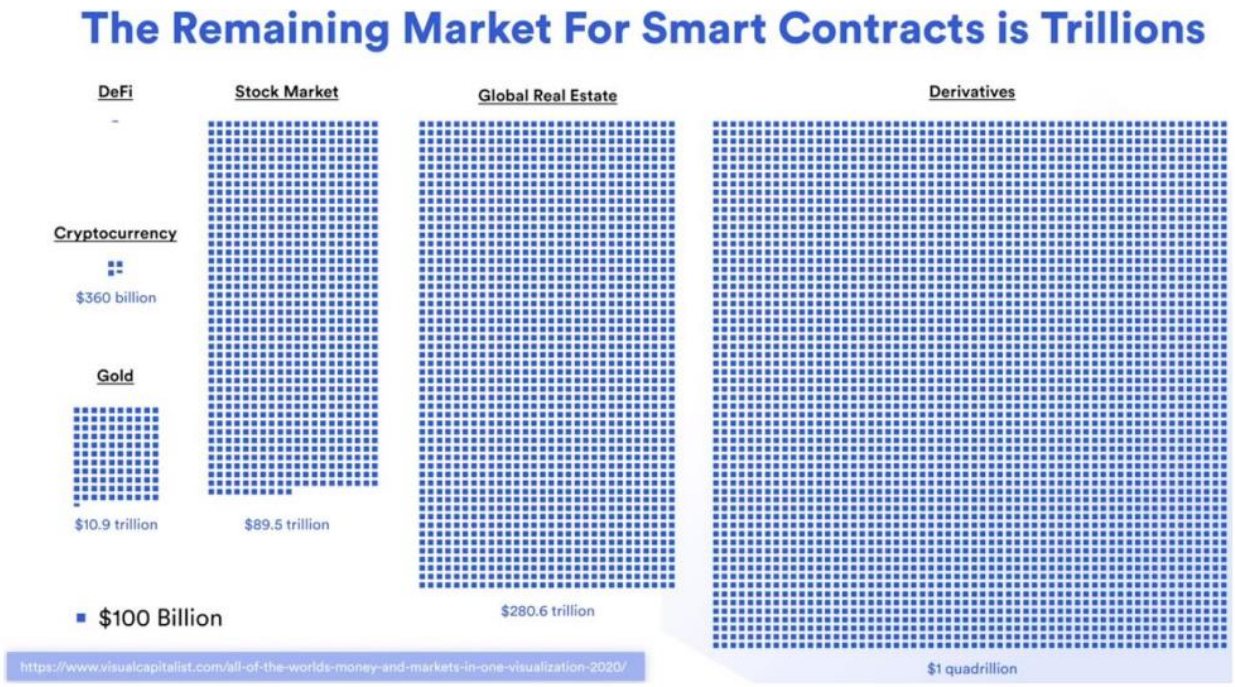

Figure 29 - Market for smart contracts

This means There will need to be trillions of dollars-worth of LINK staked against these contracts. This dynamic does not exist in Ethereum. For trust-minimized computation, prices are determined by the *amount of computation that must be performed*, *not the size of the transaction*. It costs the same amount of ETH to execute a $1 trillion dollar futures contract as it does to settle a $1 contract. This means that ETH demand, and then ETH burned via fees, can only scale with the number of transactions, not the *size* of transactions. *The Chainlink staking mechanism "value capture" via supply reduction scales with the total value of all transactions processed by the network.*

Increased demand for Chainlink services will be directly correlated with a decrease in the free float supply. As smart contract operators must pay for all LINK services – Market Data, VRF, Keepers, CCIP, Enterprise Abstraction Layer, Proof of Reserves, etc. – there will be a constant demand which will push price up. Because APYs do not diminish as more entities stake, there will be no incentive for node operators to ever un-stake their LINK tokens. Node operators will continue to earn LINK, and re-stake it in new contracts to earn more fees. This means LINK supply will be highly inelastic, even with increasing demand as smart contracts are globally adopted. Unlike a commodity resource where the supply side is elastic (oil companies can invest in more fracking plants/rigs if demand increases), there is a *finite supply of LINK tokens*. The supply side is fixed – I can't think of any similarity to this in the physical world. Even gold inflates at around 1.8% per year as mining companies expand their operations and get access to better technology. This leads me to the Node Wars.

4.3.3 The Node Wars

As discussed earlier, smart contract operators select chainlink node operators based upon reputation scores and collateral requirements. In a recent presentation, Chainlink CEO Sergey Nazarov described how the reputation scores of the best nodes are all approaching a perfect 100%. As more and more node operators establish high reputation scores by implementing all the best security practices and never failing to satisfy their SLA agreements, the amount of collateral node operators must stake is what will become the differentiating factor in what node operators are selected for jobs.

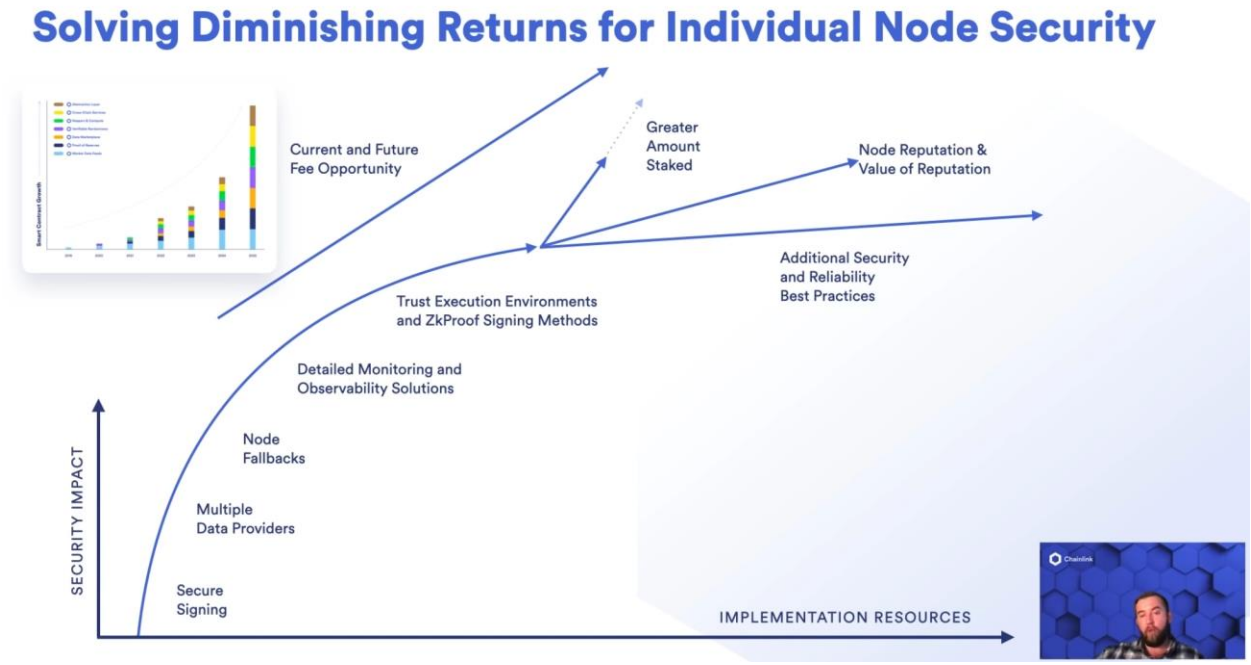

Figure 30 - Greater Amount Staked will become differentiating factor amongst highly reputable node operators

This means the LINK token is what enables entities to the future cash flows of the Chainlink network. If one owns 1% of the LINK tokens, they will own 1% of the total present and future cash flows of the Chainlink Network. Because LINK does not have diminishing yields as more entities stake, there is no incentive mechanism for node operators to sell their LINK, other than to take profits to pay for general life expenses. Due to the recent court case which established Staking Profits as Property, there is an increasingly likelihood staking yields in the form of a token won't be taxed as income at receipt [21]. This means there won't be a mechanism in place which will force larger staking entities to sell more than smaller entities. The result: The Node Wars. Already partnered with Google, Oracle, Intel, Amazon AWS, JPM, and SWIFT, likely partners from banks like CitiBank and Bank of America (and any other SWIFT bank), and current node operators T-Systems, Swisscom, The Associated Press, and Accuweather, there appears to be significant interest in monetizing one's data via running a Chainlink node. This will eventually become self-evident, leading to a race to accumulate as many LINK tokens as possible. Whereas Ethereum is set for a *90% reduction in issuance* [22], leading to a deflationary token, I believe Chainlink is set for a *90+% reduction in the total free float supply*. If node operators do not re-stake their LINK profits, their ownership in the network and hence staking revenue must necessarily decrease, assuming constant network cashflow. To maintain one's ownership in the network, one must never sell their LINK.

In a recent Twitter Spaces with the Jonny Huxtable (Founder, LinkPool) and Mark Richardson (Research at Bancor) they discussed how they expect more than 99.5% of LINK to be staked. This presents issue with DEX liquidity (which was the topic of the space), but regardless, I reiterate the founder of the leading Chainlink staking pool protocol that is funded directly by the Chainlink team said that he expects more than 99.5% of LINK to be staked.

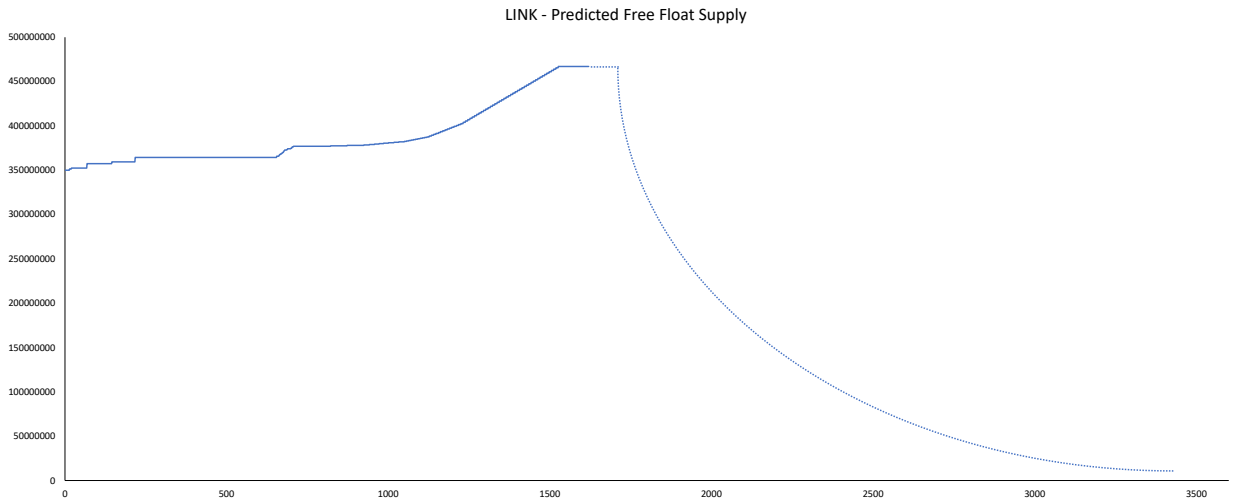

Figure 31 - Chainlink free float supply is set to decrease substantially

4.4 Chainlink Conclusion

As previously discussed, the cost of financial market and other forms of data should not decrease substantially over time. As adoption of smart contracts grow, Chainlink network revenue is going scale almost linearly with number of calls. This is opposite to Ethereum and other L1s, as previously discussed, as over time the cost per transaction is going to decrease.

With respect to number of transactions, as a blockchain-agnostic oracle network, the Chainlink protocol has exposure to every enterprise system backend, L1 blockchain, L2 blockchain, and permissioned/private blockchains. Nearly all smart contracts require access to external data or some service Chainlink provides. Their surface area for smart contracts is necessarily greater than any single L1 blockchain. I fully expect Chainlink to perform as many or more transactions than any blockchain in the future.

Although the total fees generated by all Layer 1 and 2 protocols could very well be greater than the fees generated by Chainlink, I think it is a very strong bet that Chainlink will generate more fees than any other protocol. With future advancements to Ethereum (EIP-4844 and Danksharding), fundamental advancements in L1 blockchain technology or other protocols (such as Multi-Party-Computation), I could very easily be underestimating how deflationary trust-minimized computation is as well.

Not only will Chainlink likely generate more cash flow than any L1 or L2 network, but the staking yield for Chainlink node operators does not diminish as more entities stake. One's ability to access the future cash flows of the Chainlink network is directly correlated to the % of the network one owns. This dynamic will inevitably incentivize network participants to sparingly sell their LINK tokens. Considering the following facts:

1. *All network activities must be paid for in LINK tokens*

2. *Smart contracts are likely the future of all digital agreements as we move from a society of paper-based just-trust-me agreements to cryptographically un-breakable agreements which reduce counter-party risk to 0, remove rent seeking middleman, and reduce expenses by up to 90% for some use cases*
3. *There is a finite supply of LINK tokens*

The result will be increasing demand while supply remains totally inelastic, leading to a rapid appreciation in price while providing sustainable staking yields (as denominated in USD).

With growing demand and decreasing supply, how significantly will the price be impacted? One dollar going into an asset doesn't increase the market cap by one dollar. There is a multiple, which historically has thought to be around one cent to every dollar. In a recent paper by Gabaix and Koijen in 2020 titled: *In Search of the Origins of Financial Fluctuations: The Inelastic Markets Hypothesis*, they show this multiple could be as high as 5 dollars to every dollar, a 500x increase [25]. Traditionally, the efficient market hypothesis has always presumed transactions had very little impact on prices, and this makes sense because by definition for every buyer there is a seller. The Net money is diminimous. The real contribution by this new academic research is that it appears money going in has a much higher multiplier than anyone presumed.

Looking at the history of cryptocurrencies, I would argue this research is closer to the truth than the efficient market hypothesis. Bitcoin currently is the best returning asset of all time, and it took a little over 12 years. With that said, only small amounts of BTC are needed to send it between wallets (low demand for the token), and its supply schedule has been inflationary since existence, currently sitting around 1.8%. Unlike Bitcoin, the LINK token must be purchased to utilize the network (creating significantly more demand), and once staking is released the LINK token will be significantly more deflationary than Bitcoin. I believe it is fair to say prices will be highly reflexive to the upside assuming constant demand for the LINK token. The Abstraction Capital Chainlink Investment Thesis explains in great detail where this demand will come from.

5 Conclusion

I believe it is incredibly important to understand the steady state operation of various cryptocurrencies on a long-term time horizon because ultimately every cryptocurrency will be competing with one another whether they like it or not. Markets are the continuation of evolution by other means. If a cryptocurrency, or some other digital asset, does not provide superior performance across at least one axis of utility than others, I believe it will ultimately die.

Although I have taken a bearish stance on Bitcoin's relative performance compared to other cryptocurrencies, I want to note that I am still bullish on Bitcoin relative to fiat currencies and CBDCs for the next decade. Bitcoin has by far the strongest network effect, and clearest narrative of any cryptocurrency. If we have entered a period of secular inflation, I believe it is only a matter of time until Bitcoin is no longer seen as a risk asset, and instead as a true uncorrelated inflation hedge. Although Bitcoin is non-performant, it has the strongest decentralization and censorship resistance of any cryptocurrency. To me, this is the main axis where Bitcoin is the champion. It's pseudonymous creator, Satoshi Nakamoto, remains unknown and has not moved a single one of his Bitcoin tokens. With no funding or token pre-mine, Bitcoin was released to the world where all people had an equally fair chance to mine it. Finally, with the most steadfast developer community, Bitcoin is the most difficult protocol to fork.

I believe smart contracts are the game changing technology which will enable the 4th Industrial Revolution. Smart contracts are set to disrupt any business which act as 3rd party intermediaries some class of transactions. The market size includes finance, insurance, global trade, and more. Not only will they act as the impetus for a global, transparent, and fair financial system, but they will also enable the interoperability of agents within the autonomous economy. Their potential to generate cash flow is enormous. The base layer infrastructure required for smart contracts will capture the most value from this shift. Every smart contract requires and on-chain and off-chain component.

With respect to the on-chain components, I believe Ethereum and other winning layer 1 and 2 protocols will perform incredibly well. The market for trust-minimized computation is enormous. When one account for the industries set to be disrupted, as well as the ever-expanding demand for software-based services, it is easy to see why smart contract protocols are a good bet. They provide a necessary service for Web 3.0 and will capture value proportional to usage. Just as the cloud service providers of today are cash-flow monsters, so will the winning L1 and L2 protocols.

Ethereum, to me, is the best bet because as the most secure blockchain its native token ETH will retain a monetary premium. If we live in a future with tens-of-thousands of alt L1s and L2s which purchase their security from Ethereum, even with sharding fully live Ethereum could generate massive cashflow – allowing it to maintain a deflationary token and offer very desirable staking yields. At the end of the day, there could be a cost multiple that the ETH token captures by being the most decentralized. If this is the case, then every other L1 and L2 must compete for user transaction fees, while Ethereum monopolizes fees from every other protocol as the chain for decentralization & security.

Although I expect Ethereum to perform incredibly well, the modularization of L1 infrastructure and the rise of next generation L1 protocols will lead to a dispersion of value across many different protocols. Chainlink has a unique advantage over every existing oracle network, and an increasing likelihood it captures the entire middleware space.

Due to the non-deflationary nature of various forms of data, the Chainlink network's cash flow will continue to scale near linearly with the number of transactions. With the release of the Enterprise Abstraction layer and CCIP, Chainlink will become the standard Layer 0, connecting all systems with each other. Due to the staking mechanism, the token will continue to capture value via supply reduction in a relationship which scales with the total value secured by the network. As a result, I expect Chainlink to return a higher yield than any Proof of Stake protocol and become the largest cryptocurrency by market cap in the digital asset era.

Daniel Shapiro (with help from Nelson Morrow)
Chief Investment Officer
Abstraction Capital

6 Disclaimer

Nothing written in this paper should be considered financial advice by Abstraction Capital. Invest at your own risk, and never more than what you can afford to lose.

7 Works Cited

[1] https://economics.princeton.edu/working-papers/on-the-instability-of-bitcoin-without-the-block-reward/

[2] https://micky.com.au/lightning-network-returns-just-48-a-year-for-1m-locked-up/

[3] https://blog.ethereum.org/2021/05/18/country-power-no-more/#:~:text=In%20total%2C%20a%20Proof%2Dof,(around%202100%20American%20homes).

[4] https://www.forbes.com/sites/greatspeculations/2021/07/06/bitcoin-mining-uses-a-higher-mix-of-sustainable-energy-than-any-major-country-or-industry/?sh=505de3164cc9

[5] http://www.arijuels.com/wp-content/uploads/2013/09/PoW.pdf

[6] https://www.youtube.com/watch?v=HWg731-3id8

[7] https://beaconcha.in/

[8] https://www.oneriveram.com/research : ETHEREUM: FUTURE OF FINANCE: 10/2021

[9] https://blog.lido.fi/how-lido-works/

[10] https://watchtheburn.com/

[11] https://vitalik.ca/general/2021/12/06/endgame.html

[12] https://techpolicyinstitute.org/publications/miscellaneous/cloud-computing-co-invention-for-the-masses/

[13] https://forum.anchorprotocol.com/t/anchor-oracle-price-discrepancy-on-december-9th/1714

[14] https://twitter.com/anchor_protocol/status/1469416656824799233

[15] What Really Happened To MakerDAO? (glassnode.com)

[16] https://medium.com/solana-labs/7-innovations-that-make-solana-the-first-web-scale-blockchain-ddc50b1defda

[17] https://www.weforum.org/whitepapers/bridging-the-governance-gap-interoperability-for-blockchain-and-legacy-systems

[18] https://www.youtube.com/watch?v=1uxF4Q6_glY

[19] https://blockworks.co/in-second-largest-defi-hack-ever-blockchain-bridge-loses-320m-ether/#:~:text=Wormhole%20is%20a%20protocol%20that,Smart%20Chain%2C%20Avalanche%20and%20Polygon.

[20] https://polynya.medium.com/how-ethereum-scales-simplified-9f42f43b6bb5

[21] https://blockworks.co/fate-of-millions-of-taxpayers-hangs-in-balance-of-irs-crypto-staking-case/

[22] https://squish.substack.com/p/ethereum-the-triple-halving?utm_source=url

[23] WEF_Digital_Assets_Distributed_Ledger_Technology_2021.pdf (weforum.org)

[24] https://twitter.com/epolynya/status/1504723695004119041

[25] https://www.q-group.org/wp-content/uploads/2020/10/Inelastic-Markets.pdf

[26] https://twitter.com/pseudotheos/status/1504457560396468231

	Initial Stake	Epoch 1	Epoch 2	Epoch 3	Epoch 4	Epoch 5
	10	10.20	10.40	10.61	10.82	11.04
	20	20.40	20.81	21.22	21.65	22.08
	30	30.60	31.21	31.84	32.47	33.12
	40	40.80	41.62	42.45	43.30	44.16
Total ETH Staked	100	102.00	104.04	106.12	108.24	110.41
Inflation Rate	1.02					
Network Share Entity 1	10%	10%	10%	10%	10%	10%
Network Share Entity 2	20%	20%	20%	20%	20%	20%
Network Share Entity 3	30%	30%	30%	30%	30%	30%
Network Share Entity 4	40%	40%	40%	40%	40%	40%