GSR

February 2023

Believe: Our Crypto Thesis

www.gsr.io

Cristian Gil, Co-Founder & Chairman

Rich Rosenblum, Co-Founder & President

Jakob Palmstierna, CEO

Brian Rudick, Senior Strategist

Matt Kunke, Junior Strategist

Punched in the gut, crypto is down but not out. We review where cryptocurrencies may be headed and why we remain supremely optimistic.

Highlights

Introduction: With rampant frauds and hacks, a precipitous fall in prices, and a general loss of trust and faith, it is the perfect time to reassess our views on cryptocurrencies. In what follows and with much of the pessimism driven by the decline in price, we analyze the drivers behind the recent price action and what they may imply for the future of crypto. Subsequently, we ponder various blockchain/crypto analyses and indicators - use cases and benefits, mental models, underlying fundamentals, key challenges, and areas of particular hope - to ascertain different perspectives and takeaways on what the technology may ultimately become. Finally, we offer our updated thesis on the space and our view as to when it may get there. Therapeutic for sure, but we also hope these views are helpful for those, often equipped with only a semi-complete understanding of the space, preemptively declaring crypto's demise, as well as comforting for the downtrodden, battered by the myriad risk events and irreparable action of a bad few. Maybe it's the optimist in us, but we still believe.

Thoughts on Crypto Price Action: With bitcoin down 67% from its November 2021 high and altcoins faring even worse, the putrid price action of the last 14 months has driven pessimism and despondency towards crypto from even its most ardent supporters. However, we contend that such volatile price action is normal and expected, given the nascency of the technology and related uncertainty around future cash flows and less precise valuation methodologies, lowering the fundamental information content contained in large moves. Moreover, we contend that much of the price movement has been driven by sentiment - similar to rising US software industry valuations in 2021 despite falling earnings - and by the macro environment - given the about-face in rate expectations in late 2021 - rather than a change in crypto's underlying fundamentals or its long-term outlook. The Dot-Com bust is a historical parallel where overexuberance and a supportive macro environment quickly crashed as both sentiment and the backdrop flipped, though the adoption, development, talent, and capital garnered during the boom laid the foundations for transformational technology that now touches our everyday lives. And the silver lining for crypto is that the dramatic price decline now offers significantly greater upside for those with their theses still intact - we contend that the smart money is not only HODLing but also doubling down.

Crypto's Long-Term Future State: With price a poor signal for what blockchain/crypto may become, there are a number of indicators and analyses telling of the current and future state of the industry, such as:

- Use Cases & Benefits: Blockchains bring about many use cases and benefits not possible with other technologies. First, as open, decentralized networks executing code as written and storing data in a transparent and tamper-evident manner, blockchain technology allows for the removal of intermediaries by replacing them with autonomous, trustless code, such as in decentralized finance. Second, unlike traditional finance that is built on antiquated rails, blockchain technology reimagines the rails themselves to allow for permissionless value exchange with near-zero costs and near-instant settlement at any second of any day. Lastly, blockchain technology enables new paradigms around governance (e.g., DAOs), ownership (e.g., NFTs), and business models (e.g.,

token incentives). These revolutionary use cases and benefits should fuel continued adoption and development.

- Mental Models: Mental models can help one better understand complex concepts and offer insights into what may lie ahead. One particularly pertinent mental model is that of the web, with blockchain/crypto powering its next phase. Indeed, web1 was characterized by static web pages connected by hyperlinks and controlled by businesses (i.e., the read-only web), while web2 ushered in dynamic, user-generated, community-centric web pages (i.e., the read-write web). Now, web3, using blockchain technology and tokens, is built, owned, and operated by its users rather than big tech (i.e., the read-write-own web). A second mental model is that of computer evolution, where early corporate mainframes were owned and used by large entities, and later gave rise to personal computers owned and used by individuals. Now, blockchain technology is ushering in the era of the public computer, a virtual computer existing nowhere and everywhere, owned by no one but used by all. These next iterations of the web and the computer may just be their biggest ones yet.
- Underlying Fundamentals: Another method to assess the current and future states of crypto is to examine its long-term underlying fundamental trends. Adoption and usage, for example, continue to increase despite the bear market, with the number of crypto users up ~40% over the course of 2022 and total transactions on Ethereum and its layer twos up a combined 30% in 4Q22 versus 4Q21. Development continues to increase as well, with the number of verified smart contracts deployed up 50% in 2022 and the number of full time crypto developers up 8% year-over-year as of January 2023. And despite the well-publicized layoffs, employment remains well above where it was just a few years ago, with employee counts up at most key crypto companies. Lastly, the total amount of venture capital invested in 2022 roughly matched that of the prior year, and while the pace of deployment has slowed, the $22b of funds raised last year by VCs to invest in crypto/web3 companies provides plenty of dry powder to fuel the industry for years to come. These trends amount to long-term secular expansion.
- Key Challenges: Another way to assess crypto's long-term prospects is to examine whether its main challenges may be overcome. The lack of regulation is a key challenge for centralized crypto services; however, many jurisdictions are either close to adopting comprehensive regulatory frameworks or are actively thinking about how to do so. Risks around safety and security cannot be understated, though efforts to lower smart contract risk, improve the custody experience, and reduce scams are underway. UI/UX remains particularly clunky, though many are working to abstract away the blockchain component, with efforts around account abstraction, new primitives/utilities, mobile accessibility, and privacy/interoperability. And there is a renewed focus on real utility over Ponzinomics, all suggesting that crypto will overcome these formidable challenges over time.
- Areas of Particular Promise: Cutting-edge areas may offer the opportunity to onboard large swaths of the population, portending well for the industry. Zero-knowledge proofs, for example, allow one to prove that a statement is true without revealing any other information and will usher in cloud-scale decentralized computation, anonymous payments, and new identity constructs, to name a few. And within identity, a new decentralized paradigm will enable users to own, control, and profit from their identity and data with greater privacy and security and without the need for centralized parties. Modular blockchain protocols will separate and optimize each of the core blockchain functions of execution, consensus, settlement, and data availability to achieve high security, speed, and decentralization all at once and enable mass adoption. And decentralized hardware networks will incentivize physical infrastructure development, put otherwise idle resources to work, and provide a worthy challenger to big infrastructure oligopolies.

Conclusion: The numerous risk events of the past year and precipitous drop in token prices have put cryptocurrency shortcomings on full display and have led to widespread dejection across the space. Still, we contend that large price declines are normal and expected, given the nascency of the industry, and that price action of the last two years was driven more by sentiment and macro conditions than by a change in underlying fundamentals or the ultimate outlook for what crypto may become. Indeed, when examining various blockchain/crypto analyses and indicators - use cases and benefits, mental models, underlying fundamentals, key challenges, and areas of particular hope - the future looks exceptionally strong. It won't happen overnight, as past episodes of technology adoption and changes in consumer behavior took decades to play out, but the opportunity is massive, with global crypto users representing just 5% of the total population and the cryptocurrency market cap representing just 0.8% of that of both equities and bonds. So despite the atrocious year that 2022 was, the future of crypto has never looked so bright. In short, we still believe.

Table of Contents

Details

As tradfi converts, we have received nonstop DMs from former colleagues proclaiming, sometimes triumphantly, the death of crypto. After the debacle of a year that 2022 was and with consideration for the astute possibility that they may indeed be correct, we felt it the perfect time for reflection. In what follows, we examine the drivers behind recent price action. We then employ various blockchain/crypto analyses and indicators such as its use cases and benefits, mental models, long-term trends, key challenges, and areas of particular hope to analyze where the industry stands and what may lie ahead.

Before diving in, a brief review of how we got here.

2021 - What a Year!

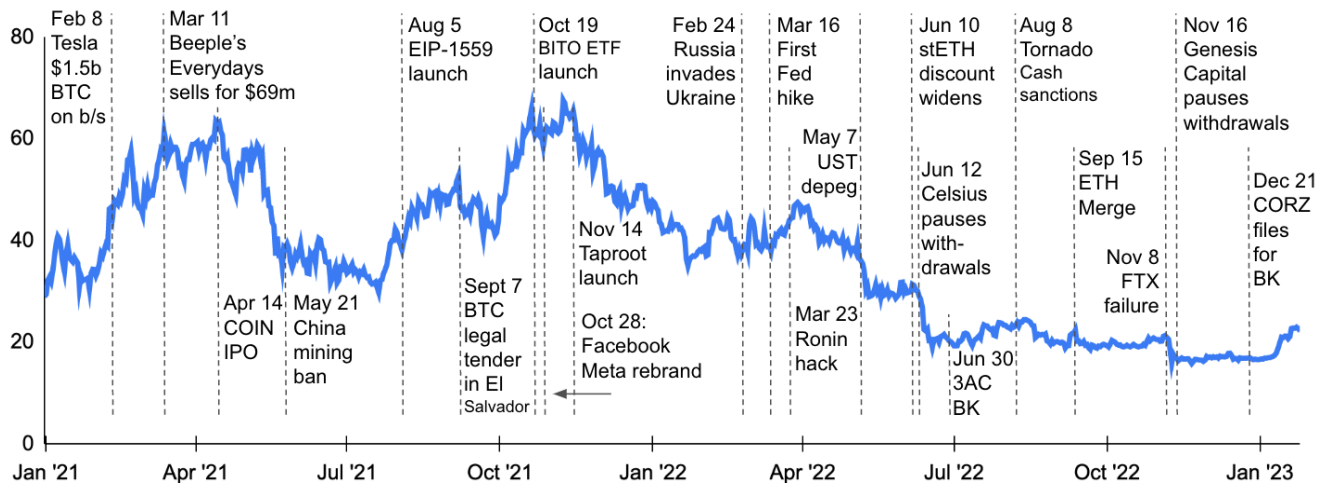
Building on the foundations of years past and with continued tailwinds from the pandemic and related government assistance programs, 2021 was a historic year for Bitcoin and cryptocurrency more generally. From Tesla's addition of BTC to its balance sheet, Beeple's $69m NFT sale, Coinbase's IPO, El Salvador declaring BTC legal tender, and the US SEC approving a futures-based bitcoin ETF, cryptocurrencies entered the cultural zeitgeist like never before. Key growth sectors took off, including alternative smart contract blockchains, NFTs, stablecoins, DeFi, GameFi, and even meme coins. By the numbers, the total crypto market cap nearly tripled, Bitcoin's hash rate doubled from its post-China ban bottom, crypto venture investment totaled more than all prior years combined, and crypto spot trading volume increased ~700%. Oh, the days of yore.

2022 - It's Been a Year.

Though 2022 witnessed many positive developments highlighted by Ethereum's transition to proof-of-stake, last year, with risk events abound, was quite simply the antithesis of 2021. In May, a shaky macro backdrop, self-reflexive stability mechanism, and artificial mint-burn limits brought down popular layer one blockchain and algorithmic stablecoin issuer Terra Luna. Next up was Celsius, an outright fraudulent centralized borrow/lend provider that gambled depositor money via degen strategies like the levered staked ETH trade, quickly followed by crypto hedge fund Three Arrows Capital, which found itself with too much leverage and too many losing trades. And recently, prominent derivatives exchange FTX so sanctimoniously violated user trust and the law by feeding deposits to its money-losing predatory prop shop Alameda Research, pushing the $32b exchange into bankruptcy within a matter of days. And this is in addition to the $3.5b+ of hacks that occurred, including Ronin, Wormhole, Nomad, Beanstalk, Wintermute, Elrond, Horizon Bridge, Binance Bridge, and Mango Markets. The dejection on Crypto Twitter is palpable, and the loss of trust will take years to overcome.

All that said, things are generally never as high or as low as they seem at the time. So without further ado, let's dig in.

Exhibit 1: Major Cryptocurrency Events, Last Two Years, vs. BTC Price, $k



Source: Santiment, GSR

Analyzing Price Action

With bitcoin down 67% from its November 2021 highs and altcoins faring even worse, the putrid price action of the last 14 months has driven pessimism and despondency towards crypto from even its most ardent supporters. However, we contend that such volatile price action is normal and expected, given the nascency of the technology, and that such price movements have been driven more by sentiment and macro factors than by a change in crypto's underlying fundamentals or its ultimate outlook.

Examining historical price moves puts the current decline in perspective and makes it appear somewhat pedestrian. Putting bitcoin's price on a logarithmic scale displays percentage changes in a linear fashion, representing percentage changes equally regardless of price (i.e., a move from $10 to $50 appears the same as a move from $10,000 to $50,000), with such charts more appropriate for displaying long-term trends and exponentially increasing data series. While the latest downturn is certainly notable, it does not stick out as catastrophic in the context of bitcoin's full history. And while it may feel worse going from $67,500 in November 2021 to ~$23,500 currently, the move is not too dissimilar to when bitcoin went from $732 to $321 in 2014. In fact, the 77% drawdown from bitcoin's local peak on November 9, 2021 to its local trough on November 21, 2022 doesn't even rank in its top three drawdowns, which are the 93%, 85%, and 83% drawdowns that occurred largely in 2011, 2014, and 2018.

Bitcoin's Historical Price Movements

Bitcoin Price - Logarithmic Scale

Historical Bitcoin Drawdowns Ranked

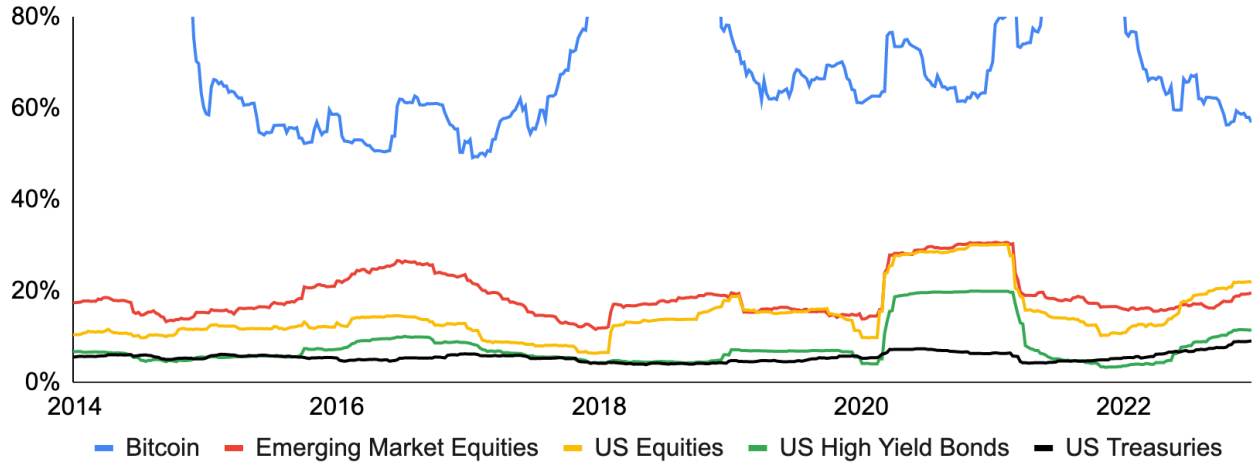
Rank	Start Date	Trough Date	Recovery Date	Peak to Trough, Days	Peak to Recovery, Days	Draw-down
1	Jun 9, '11	Nov 18, '11	Feb 20, '13	162	622	-93%
2	Dec 5, '13	Jan 14, '15	Feb 23, '17	405	1,176	-85%
3	Dec 17, '17	Dec 15, '18	Nov 30, '20	363	1,079	-83%
4	Nov 9, '21	Nov 21, '22	TBD	377	TBD	-77%
5	Apr 10, '13	Jul 6, '13	Nov 5, '13	87	209	-71%
6	Apr 14, '21	Jul 20, '21	Oct 19, '21	97	188	-53%
7	Nov 7, '10	Dec 9, '10	Jan 14, '11	32	68	-49%
8	Jul 19, '10	Jul 25, '10	Oct 9, '10	6	82	-41%
9	Feb 10, '11	Apr 4, '11	Apr 17, '11	53	66	-37%
10	Jun 12, '17	Jul 16, '17	Aug 5, '17	34	54	-36%

Source: Glassnode, GSR

Such volatility, we contend, is due to two reasons, with the first related to the visibility and certainty of future cash flows. In its purest sense, an asset is worth the present value of its future cash flows, and different asset classes have very different certainty and predictability of such cash flows. On one side of the spectrum are assets with near-certain future cash flows, such as a US Treasury, while on the other side are assets with extremely difficult-to-predict future cash flows, such as an emerging tech company or seed stage startup. Assets on the former side of the spectrum will see cash flow expectations change little, making their price much less volatile, while assets on the latter side will often see cash flow expectations change drastically, leading to large price swings. Crypto fits squarely on the latter side of the spectrum, leading to its greater volatility.

In addition, given their differing levels of cash flow predictability, assets on either side of the spectrum utilize very different valuation methodologies that have different levels of precision relative to more slow-moving underlying fundamental value. Valuation on the former end, for example, is simple to calculate given near-certain cash flows, such as with the US Treasury bond where the only debatable input is the discount rate. Valuation for the latter side of the spectrum, however, is much more difficult to discern and often eschews cash flows altogether in favor of alternative measures indicative of but less directly related to future cash flows, such as the total addressable market for the emerging tech company or betting on its founders for the seed stage startup. These valuation methodologies are much less precise and have much wider confidence intervals, leading to greater volatility in the valuations (i.e., prices) themselves. All in, the nascency of the technology leads to greater volatility in cash flow expectations that when combined with less precise valuation constructs, results in greater volatility and lowers the information content contained in extreme price moves.

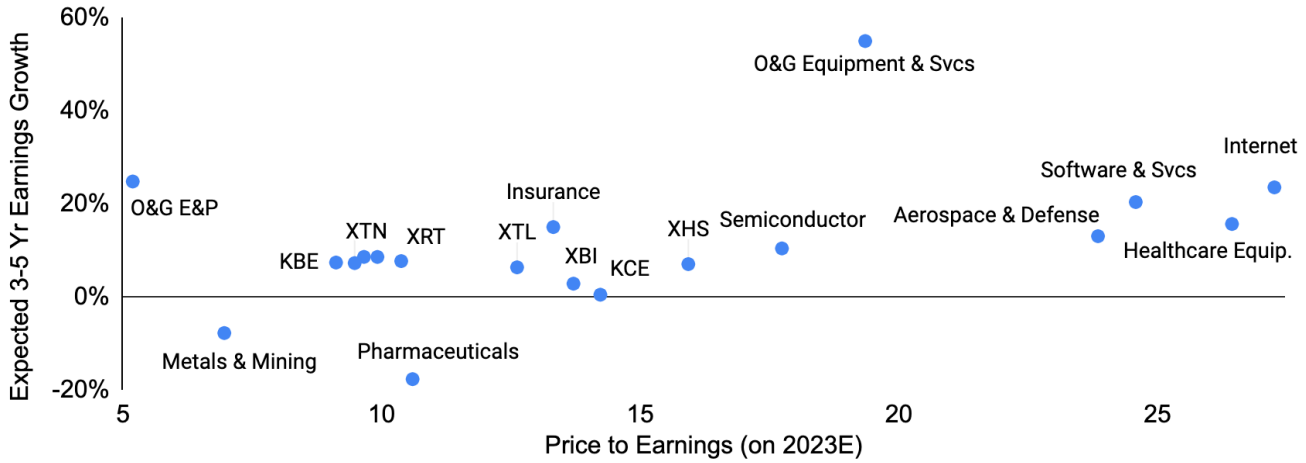
Rolling 52-Week Annual Volatility for Various Asset Classes



Source: Yahoo Finance, GSR
Note: We limit the Y-axis to show more detail for the other asset classes. We use the following ETFs in our calculation: VWO for Emerging Market Equities, SPY for US Equities, HYG for US High Yield Bonds, and IEF for US Treasuries.

In addition to lower information content in large price moves due to innately high volatility, we contend that much of the price action of the last two years was driven by sentiment and macro factors rather than changes in cryptocurrency underlying fundamentals or its long-term outlook. While blockchain/crypto as an industry doesn't currently have revenue or earnings per se, one way to think about this is to decompose price into earnings and the multiple, with near-term earnings determined wholly by fundamentals and the multiple determined by both fundamental and non-fundamental factors such as sentiment and rates (a multiples analysis is simply a short-hand discounted cash flows analysis, so the multiple does capture out-year earnings beyond the near-term earnings used in the decomposition). One notable takeaway is that less mature industries with greater expected future growth tend to have higher multiples, meaning that more of their value is ascribed to the multiple - something that is at least partially determined by sentiment. In fact, plenty of academic studies have found early-stage companies/industries to be particularly sentiment-driven, such as this one that concludes "stocks of low capitalization, younger, unprofitable, high volatility, non-dividend paying, growth companies (...) are likely to be disproportionately sensitive to broad waves of investor sentiment." Crypto, with nearly all of its potential earnings far in the future, sits squarely here, causing the preponderance of its value to be determined by its sentiment-impacted multiple.

Industry Multiples vs. Expected Growth

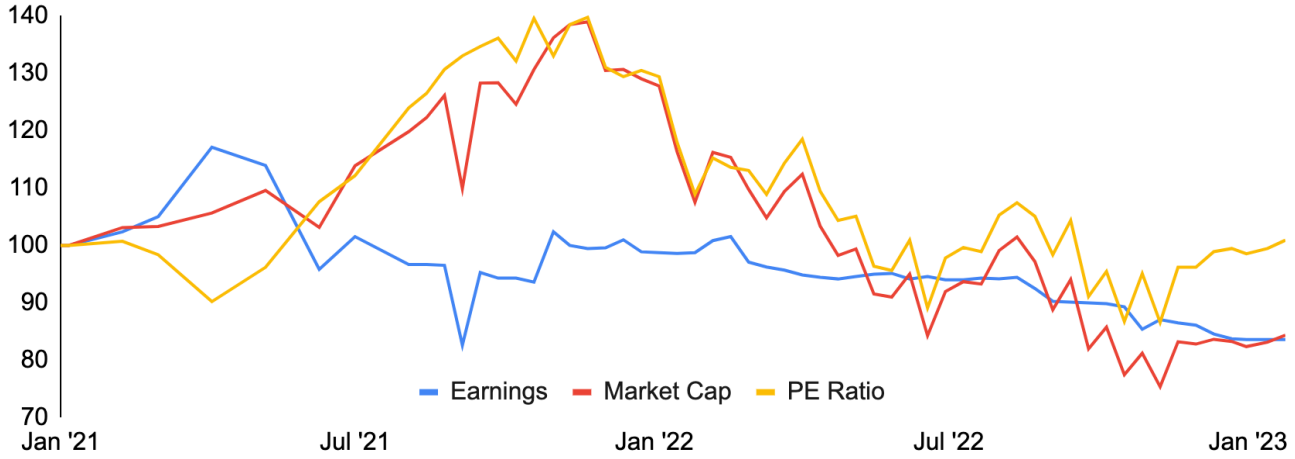


Source: SSGA, GSR

Note: Data as of January 20, 2023. We use the following SPDR S&P industry ETFs: Oil & Gas Equipment & Services (XES), Oil & Gas Exploration & Production (XOP), Internet (XWEB), Software & Services (XSW), Healthcare Equipment (XHE), Insurance (KIE), Aerospace & Defense (XAR), Semiconductor (XSD), Homebuilders (XHB), Regional Banking (KRE), Retail (XRT), Bank (KBE), Transportation (XTN), Health Care Services (XHS), Telecom (XTL), Biotech (XBI), Capital Markets (KCE), Metals & Mining (XME), and Pharmaceuticals (XPH).

While crypto sentiment and price are interdependent (is price down because sentiment has fallen or has sentiment fallen because price is down?), we can examine more mature businesses with more easily aggregatable earnings, such as the US software industry, to determine reasons for changes in price. As denoted by the blue line below, the software industry experienced steadily declining earnings throughout 2021, though its price, driven by gradual multiple expansion throughout the year, continued to increase. And with no change in rate expectations for the vast majority of the year, we can conclude that such price action was driven primarily by increasingly positive sentiment as investors awarded a higher multiple to the declining earnings stream. As another fast-growing area of technology, we highly suspect that extensive sentiment-driven multiple expansion drove 2021's phenomenal price increases. Put another way, the underlying technology and potential for what cryptocurrencies may become did not triple in 2021, like the total crypto market cap did, but by the same logic, it did not regress by two-thirds as suggested by 2022 price performance.

US Software Industry: Price Decomposition - Earnings vs. PE Multiple

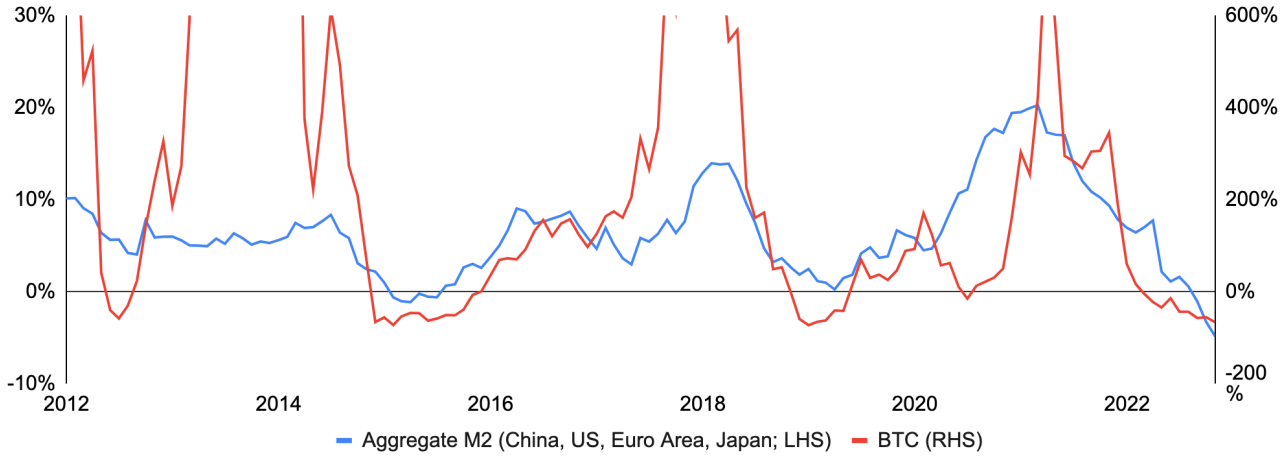


Source: SimplyWall.St, GSR

In addition to sentiment, the macro environment can have a drastic impact on prices. Low rates and high liquidity, for example, often lead to inflated valuations, both as the present value of future cash flows increases due to a lower discount rate and as additional demand pushes up prices as capital searches out yield, often ending up in speculative assets. This is exactly what we witnessed in 2021, with a particularly supportive macro backdrop with near-zero rates and continued quantitative easing causing nearly all major equity indexes to increase and cryptocurrencies to boom. However, as 2021 came to an end, central banks no longer viewed inflation as transitory and communicated that they would soon remove monetary accommodation, with rising rate expectations both reducing the level of expected future cash flows given lower expected economic growth and lowering the present value of such cash flows given higher discount rates (in addition to increasing the cost of leverage and raising the attractiveness of safer fixed income investments). Equity markets quickly fell in response, and crypto tumbled.

While hard to fully disentangle, the price of bitcoin and economic cycles, shown below as proxied by global liquidity in the form of the M2 money supply, do appear to be related, with bitcoin performing extremely well in times of accelerating global liquidity growth and performing poorly when liquidity growth slows. Note two other items: First, the price of bitcoin often increases many times over during cycle peaks given exuberance at the top (i.e., extreme moves in sentiment / the multiple) and a still relatively-small market capitalization. Second, cryptocurrencies experienced many idiosyncratic positive catalysts in 2021 and negative risk events in 2022, likely exacerbating these macro-induced moves.

Global Liquidity vs. Bitcoin Price, Year-Over-Year Growth

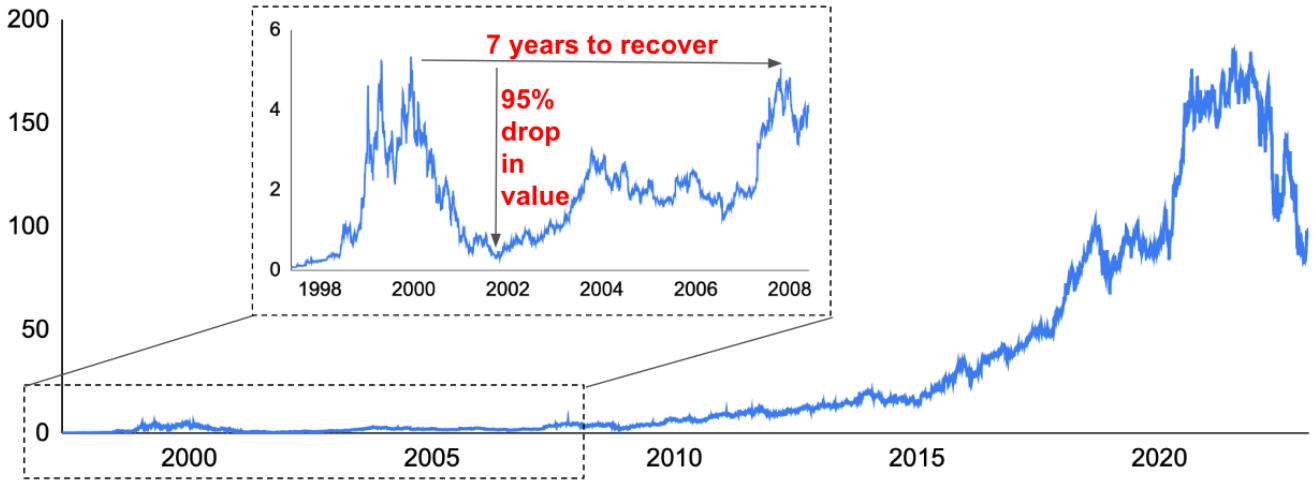


Source: The People's Bank of China, Federal Reserve, European Central Bank, Bank of Japan, Investing.com, Glassnode, GSR.
Note: Converts local currency M2 to US dollars and aggregates before taking year-over-year growth. Note that different countries may define M2 slightly differently, but the general concept of M2 is that of a measure of the money supply that includes cash, checking deposits, and non-cash assets that can easily be converted into cash.

The collapse of the Dot-Com bubble in the early 2000s is an intriguing historical parallel to the state of crypto today. The launch of Netscape's web browser in 1994 and its subsequent IPO in 1995 illuminated the web's potential to millions of people for the first time and ushered in an era of speculative euphoria. Many new internet companies quickly appeared pitching more efficient approaches to legacy business models, with perhaps none more prominent than 'eCommerce.' The number of IPOs skyrocketed in the late 90s, with many generating staggering one-day returns that further perpetuated the hype cycle.

It was, however, not to last. Despite the potential for transformational growth, the sector quickly became oversaturated with low-quality businesses. Moreover, the boom in internet stocks arose during a pro-cyclical backdrop featuring fresh capital gains tax cuts and low-interest rates, but it quickly began to unravel as monetary conditions tightened. The bubble burst in March of 2000, with the NASDAQ subsequently falling 77% and internet stocks fairing even worse. Amazon, for example, fell 95% from its peak and took a full seven years to recover. The good news, however, is that many of today's tech juggernauts, now a cornerstone of our everyday lives, were born during this time (and Amazon's stock has returned ~328x since its 2001 low). More importantly, an increase in awareness and usage and an influx of talent and capital into the space laid and accelerated the foundation for the internet companies of today. Similar to the internet sector in the late 90s, overexuberance in crypto and a changing macro backdrop drove a meteoric rise in prices that crashed as quickly as it rose despite the technology's transformational potential. Sentiment and valuations have now been reset, but the foundations to change the world are being set in the rubble.

Amazon Stock Price Chart



Source: Yahoo Finance, GSR; chart replicated from Twitter @Melt_Dem.

With prices over the last two years in the realm of normal, expected, and due more to changes in sentiment and the macro environment than in the industry's underlying fundamentals or long-term outlook, we believe such movements have little implications for what crypto may become and are thus looking past such moves. In fact, using price to inform value, particularly for such a nascent asset, is a recipe to buy high and sell low. And with more upside potential to price targets, the smart money is doubling down.

Looking forward, we are likely in for a long winter. But the bad actors have been exposed, the fast money has been flushed, and now only true believers and builders remain. Over the near term, prices will likely move with the macro, briefly deviating as the occasional crypto-specific catalyst or risk[1] comes to fruition. But over the long-run, prices will follow fundamentals, which we tackle in the next section.

[1] In the spirit of candor, we see more near-term potential risks than possible positive catalysts. That said, we believe crypto is particularly hard to time, with the more important question being whether one believes blockchain/crypto will be bigger in ten years than it is right now, rather than trying to exactly time the market. Nevertheless, risks and catalysts include: Risks include further turmoil at industry conglomerate Digital Currency Group and the unwind of its $12b Grayscale Bitcoin Trust, ~$2.4b in bitcoin that will likely be returned to hacked Mt. Gox customers this year and potentially sold, the unlocking of staked ETH post Ethereum's coming Shanghai upgrade in March, the unlikely but catastrophic collapse of industry leaders given their sheer dominance like crypto exchange Binance with its 80% spot market share or stablecoin issuer Tether which oversees 50% of all stablecoins outstanding, centralization concerns from Ethereum's concentrated US-based validator network and other centralized components such as RPC providers/front-end hosting services, the US SEC declaring most cryptocurrencies securities, and additional large-scale hacks or frauds. Potential positive catalysts include sensible crypto regulation, a US spot bitcoin ETF approval, a large retailer like Amazon adding a crypto payment option, and additional large countries declaring bitcoin legal tender or adopting blockchain-based technologies.

Crypto's Long-Term Future State

With price out of the way, we can employ various analyses and indicators to assess the current state of crypto and examine where it may be headed. In what follows, we expound on various mental models, examine long-term underlying fundamental trends, assess whether key challenges may be overcome, and explore areas of particular hope. But first, we assess blockchain/crypto's use cases and benefits.

Use Cases & Benefits

The best tell of what a new technology may become likely starts with why one may use it in the first place and its benefits over existing alternatives, though prior to diving in, we present a basic overview of what cryptocurrencies are and how they work. While a full explanation is outside the scope of this report - see How Bitcoin Works and Ethereum's Roadmap for semi-technical yet accessible primers - the short version is as follows: Bitcoin is a network of thousands of unrelated computers around the world called nodes that simply record who paid what to whom, when, almost akin to all computers keeping the same local copy of an Excel spreadsheet. That's it. Going one layer deeper, nodes record payments of bitcoin, a digital asset by the same name, and use cryptography and a consensus mechanism to agree on valid transactions whereby nodes compete to be the first to solve a puzzle to post their proposed transactions/block to the blockchain (spreadsheet) and receive a bitcoin reward. Such a construct - an open network of unrelated nodes following code-based rules to agree on and record valid transactions without a central leader - results in Bitcoin's key properties of decentralization, trustlessness, censorship resistance, immutability, permissionlessness, and scarcity, to name a few.

While revolutionary in its own right, Bitcoin has morphed from its intended peer-to-peer electronic cash system into a store of value given technical limitations and a fixed supply, though its underlying technology forms the basis of second-generation blockchains like Ethereum. Indeed, instead of having thousands of computers around the world simply keep track of payments, nodes on the Ethereum network can also process code, known as smart contracts, adding programmability and arbitrary computation to the decentralized ledger. And with similar construction, it does so in a manner that is also decentralized, trustless, censorship-resistant, immutable, and permissionless.

As an example, imagine that you own an apartment and want to rent it out over the internet, but are hesitant to send the unknown renter your digital entry keycode prior to receiving payment, and the renter is similarly hesitant to send payment prior to receiving the digital keycode. In the real world, you might use an escrow agent as an intermediary, though you will have to both trust this intermediary and pay for the service. By contrast, one can simply deploy a short smart contract to the Ethereum blockchain, where nodes on the network monitor for state changes - whether the digital keycode and/or payment have been uploaded - and when both conditions are met, they will make the swap[2]. As seen in this example, a smart contract blockchain can not only store information but also process computation, transforming the blockchain into a decentralized, trustless computer.

While blockchains enable new capabilities and constructs so profound they are hard to organize into

[2] We use this example for simplicity but in general, data in a public blockchain is visible to all, and one would not want to use it to share a secret in plaintext.

distinct, definable categories and new innovations are sure to come about, we see the main use cases and benefits being the removal of intermediaries, the democratization of value exchange, and the enablement of new paradigms around ownership, governance, and business models. We expound on each below.

Bitcoin Properties & Blockchain Use Cases

Bitcoin Properties		Blockchain Use Cases	
Decentralized	Permissionless	Store of Value	Ownership
Trustless	Open Source	Payments	Governance
Censorship Resistant	Pseudonymous	Record of Account	Decentralized Computation
Immutable	Scarce	Identity	Many More

Source: GSR

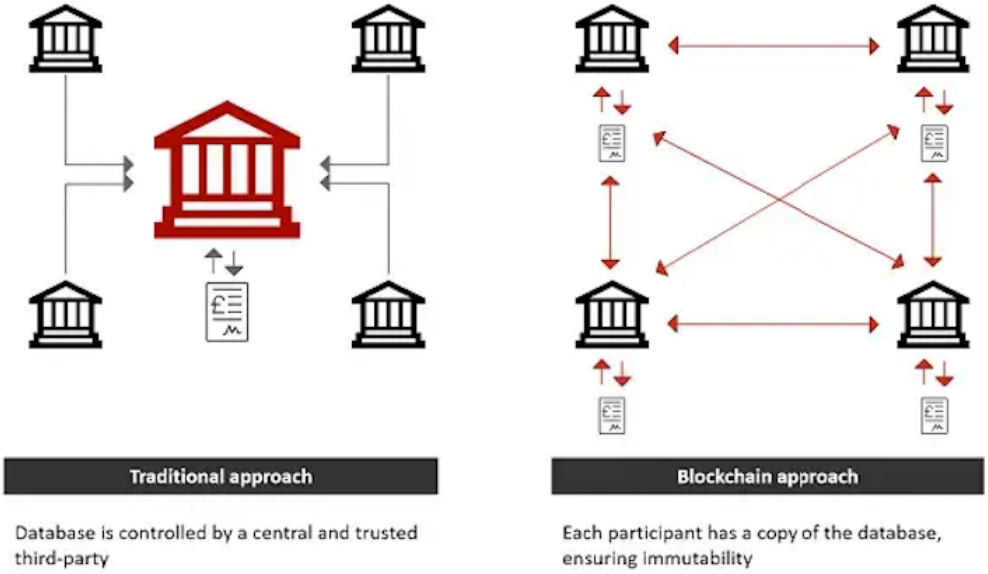
Removal of Intermediaries

Trust is foundational to nearly all aspects of society, and its enablement greases the wheels of social and economic activity. Today, we rely on a combination of laws, societal norms, and generally accepted business practices, though immediate trust at scale is still fleeting. For this, we often turn to intermediaries, though doing so requires us to trust the intermediaries, who also extract rent for their services. As an open, decentralized network executing code as written and storing data in a transparent and tamper-evident manner, blockchain technology instantly instantiates trust and removes the need for intermediaries. In other words, blockchain technology is a step change in society's trust infrastructure, enabling trustless cooperation, flexibly and at scale.

There are many areas of society today where blockchain technology can be introduced to natively manifest trust, resulting in fewer intermediaries, the removal of rent extraction, and improved efficiency. The traditional finance industry, for example, is built on mostly centralized systems of financial intermediation, with a few key parties holding the power, performing the intermediary work, and earning fees for such service. Banks allow depositors to lend to unknown borrowers, exchanges enable trade between unrelated parties, and insurance companies transfer and diversify risk from individuals to the collective. While of tremendous value, a trustless peer-to-peer network can perform the same functions without the need to trust a centralized, profit-maximizing leader and with efficiency gains going to the community. Decentralized finance (DeFi) is a great example, where borrow/lend protocols utilize crowd-sourced liquidity pools to lend against collateral locked in smart contracts, decentralized exchanges enable peer-to-peer trading between self-custodying users and trading fee-compensated liquidity providers, and DeFi insurance applications automatically verify claims via self-executing autonomous smart contracts - all in a trustless fashion and at typically lower cost than in traditional finance. Moreover, these trustless peer-to-peer marketplaces are used beyond DeFi, such as with file storage, GPU compute, 5G wireless, and more, while in the creator industry, artists and entertainers can bypass the complex incumbent system of intermediaries to sell directly to fans. Even sovereign/country-level intermediation can be contested, such as with Bitcoin's codified maximum supply challenging the currency debasement so common from today's central banks (hence why Bitcoin

is often referred to as a non-sovereign money).

Trust & Intermediaries



Source: Alejandro Reyes, GSR

Democratization of Value Exchange

The legacy financial system is built on antiquated technology, leading to high costs, long wait times, and in some cases, discriminatory practices, poor user experience, and suboptimal security. For example, ACH and remittance payments can take up to five days to transfer, credit card networks charge merchants 2-3% resulting in higher consumer prices, and a complex clearing and settlement system delays the settlement of stock trades for days after execution, all resulting in worse convenience, cost, risk, and capital efficiency. Even fintech, with innovation largely confined to the front-end, still operates on these traditional, antiquated rails on the back-end.

Blockchain technology, by contrast, innovates on the back-end to reimagine the rails themselves. Already, blockchain-based payments can occur 24/7/365 at near-zero costs and near-instant settlement. Businesses can accept digital asset-based payments with only a public key and without the need for specialized hardware or payments to issuers, merchant acquirers, and card networks. And the blockchain itself can serve as a real-time, verifiable, immutable public ledger resulting from open code executed as written to materially increase transparency and reduce disputes. In the future, financial inclusion will increase with permissionless protocols requiring only an internet-connected device to participate, user experiences will improve with key pairs serving as identification, account numbers, and passwords, and security can strengthen with private information self-custodied by the user rather than spread across innumerable institutions, companies, and websites.

Moreover, blockchain technology enables the exchange of many other forms of value and introduces new capabilities not possible with the existing financial rails. Tokenization, for example, will eventually bring the exchange and record of account benefits to nearly all other assets in addition to money, such as with blockchain-based digital forms of traditional securities known as tokenized securities. And these

speed and cost advantages introduce new capabilities and constructs, such as enabling previously-impractical micropayments to charge fractions of a penny per song streamed to better reward creators or per web page viewed to reduce DDoS attacks. Programmability will enable new capabilities, such as subsidy payments only spendable on specific categories, composability will make accepted token formats ubiquitous and usable across the digital realm, and fractionalization will improve accessibility and liquidity. These examples, with significant improvements in speed, cost, inclusion, and transparency, only scratch the surface of what's possible.

Traditional vs. Blockchain-Based Payments

	Traditional Payments	Blockchain Payments
Network	Through centralized infra / companies	Peer-to-peer
Rails	ACH, credit card networks, etc	Blockchain / internet rails
Cost	Ranges	Near-free
Speed	Ranges	Near-instant
Availability	Business hours	24/7/365
Transparency	Low	High
User info storage	By many parties	By the user
Additional features	Reversible	Programable, composable

Source: GSR

Enablement of New Paradigms around Governance, Ownership, and Business Models

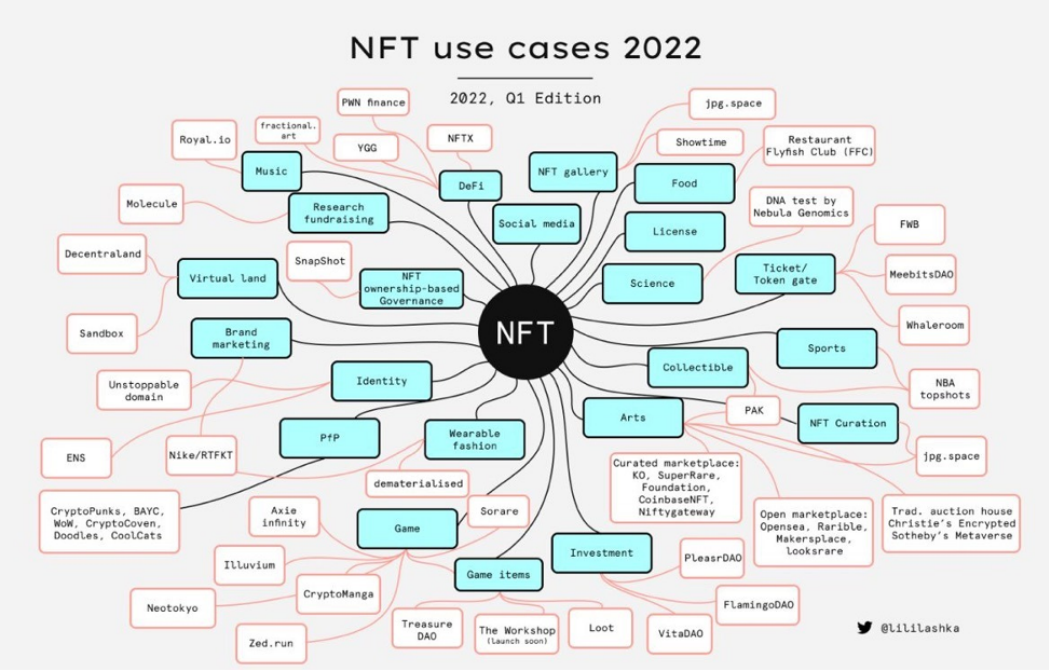
In addition to the removal of intermediaries and democratization of value exchange, blockchain technology enables new paradigms around governance, ownership, and business models. Starting with governance, self-organized online protocols and communities, often in the form of decentralized autonomous organizations (DAOs), may follow automatically-enforceable, smart contract-based rules and utilize the organization's token to enable holders to table and vote on proposals determining future activities and actions. Such community governance enables bottom-up decision-making, organization around shared goals, borderless collaboration, and transparent management. Already, community governance is used to govern protocols, fund grants, distribute creative work, direct investment, and socially unite members, and in the future, will improve civic engagement, streamline business creation and fundraising, reward early contributors, and create shared financial and social capital. Workers, unconstrained by national, regulatory, or legal boundaries, will self-define work based on true passion across multiple DAOs, enhancing productivity and motivation. Birthed by the community intent on consuming them, products and services will better match demand and align output with societal needs. And contribution-driven ownership and reward will open up opportunity and financial freedom based on true merit rather than the oft-political and bureaucratic corporate environments of today.

Blockchain technology also brings about new ownership paradigms, enabling for the first time the true ownership of digital items, both fungible and solely unique non-fungible tokens (NFTs). As blockchain-based digital representations of ownership, NFTs make digital assets as real and as permanent as objects in the physical world, bear the typical cryptocurrency benefits discussed above, and enable new constructs around content, ownership, value, and exchange. Content creators, with

output as NFTs, can sell directly to fans, price along the demand curve, monetize secondary sales, and crowdfund new works prior to creation to maximize value capture, better align to consumer preferences, and reward early supporters. NFTs will enable the metaverse, turning the current flat online social structure into virtual economies that rival and perhaps one day eclipse the real world. And the benefits of programmability, composability, and tokenization apply to ownership as well, increasing NFT utility and functionality, speeding development, and enhancing efficiency, transparency, portability, and security.

Lastly, blockchain technology and cryptocurrencies enable new paradigms in business models. For example, it's nearly impossible to create a new ridesharing service, given existing network effects, as drivers would hesitate to drive without riders, and riders would hesitate to ride without drivers. However, a new blockchain-based ridesharing protocol can reserve a large portion of newly created tokens to award to early drivers and riders, allowing early participants to benefit from the application's growth in addition to the founders and investors, effectively bootstrapping network effects. And in gaming, blockchain technology can revolutionize the business model for players, game developers, and the virtual worlds alike. For players, blockchain-based gaming enables users to truly own items, transforming in-game purchases from an expense to an asset and enabling resale and portability of items to other games. For game developers, blockchain technology expands revenue streams, moving game creators from mainly selling in-game items to overseeing a dynamic virtual economy where they can take a cut of all commerce. And the system can benefit from rich incentives to reward players for accomplishing tasks, producing content, and onboarding new users, where both gamers and developers are aligned and benefit as the game grows.

NFT Use Cases



Source: @Lililashka, GSR

With strong use cases and benefits superior in many ways to existing solutions, the continued development and adoption of blockchain technology and cryptocurrencies seems inevitable. Indeed, its use can instantly instantiate trust at scale to remove intermediaries in lieu of trustless peer-to-peer marketplaces for lower costs and increased efficiency. Payments and the exchange of value may occur 24/7/365 with near-zero cost and near-instant settlement. And community governance, true digital ownership, and new business models will be birthed, all while benefiting from programmability and composability.

Mental Models

Mental models can help one better understand complex concepts and offer insights into what may lie ahead. As such, we present two mental models for blockchain technology and cryptocurrencies below. Many of these ideas were created and/or popularized by Chris Dixon and colleagues at crypto venture firm a16z, and we highly recommend this episode of The a16z Podcast for readers interested in learning more.

The Next Iteration of the Web: Web1 -> Web2 -> Web3

Originally designed for automated information sharing between academics, the World Wide Web (web) was invented in 1989 at CERN by British computer scientist Tim Berners-Lee. The web serves as an information system enabling documents and other web resources to be accessed over the internet (yes, the internet and the web are different). And as Gen Xers can astutely attest, the web has evolved considerably since its early days. With blockchain and cryptocurrencies at the heart of its next iteration, the generally accepted phases of the web are:

Web1: The early days of the web were characterized by a small number of typically-corporate webmasters creating static, read-only content for a large number of readers. These pages, connected together via hyperlinks, allowed content consumption anywhere in the world at any time but were controlled unilaterally by the webmasters and were not responsive to their viewers. Web1 lasted until the mid-2000s and was the read-only web.

Web2: Spurred by rising internet adoption, faster internet speeds/mobile access, and the rise of social media, webpages, often in the form of platforms, suddenly became dynamic, user-generated, and community-centered. Facebook and YouTube are prime early examples. While users can now create content for the world to see, they largely do not own or monetize it. Web2 is the predominant form of the web today, and, sometimes called the participatory social web, is the read-write web.

Web3: Built on blockchain technology and with tokens enabling ownership, identity, value exchange, and coordination/incentivization, the web is increasingly being built, owned, and operated by users rather than by monopolistic tech behemoths. Users can for the first time own items in the digital realm, possess and profit from their digital identity, utilize wholly native payments, and build, govern, and own platforms they use via decentralized governance. Coined by Polkadot founder Gavin Wood in 2014, web3 is decentralized, permissionless, trustless, and censorship-resistant, and is the read-write-own web.

Digging into web3, anyone can create a decentralized application running the gamut from financial applications like exchanges and lending protocols, entertainment applications like gaming and video/music streaming, social applications like art collectives and common interest clubs, and infrastructure and business services applications like storage, compute and others, just to name a few - and these protocols are accessed permissionlessly and execute trustlessly per open-source code. Moreover, the decentralized application can create tokens to facilitate exchange, such as for payment within the application, to offer community governance with token holders able to propose and vote on future protocol initiatives, and to reward value contribution/incentivize behavior with tokens allotted to high contribution community members and early users to accelerate development and use. And over time, such protocols can morph into community-owned-and-governed economies, eliminating the boundaries of physical distance, removing barriers to education and opportunity, and enabling earning, consumption, and socialization. While admittedly hard to conceptualize, web3 is likely to be the web's biggest iteration yet.

Web1, Web2, Web3 Comparison

	Web1	Web2	Web3
Dates	1990-2004	2004-present	2014-present
Description	Read-Only	Read-Write	Read-Write-Own
Focus	Corporations	Communities	Individuals
Base	Homepages	Social Media Platforms	Blockchains
Content	Static	User Generated	User Owned
Owner	Corporates	Big Tech	Individuals
Companies	Netscape, Yahoo, Alta Vista	Facebook, YouTube, Twitter	Ethereum, Uniswap, PleasrDAO

Source: GSR

The Next Computer: Corporate Computer -> Personal Computer -> Public Computer

While humans have been using calculation devices for centuries, one way to delineate computing movements is by who owns and uses the device. By this definition, the two most notable computer movements have been around corporate ownership and use with the mainframe computer and individual ownership and use with the personal computer. And with blockchain technology bringing about a virtual computer owned and used by all, the era of the public computer is underway. In more detail, these computing movements are:

Corporate (Mainframe) Computers: Mainframes are large computers used by organizations for critical applications like data and transaction processing. Many consider the start of the mainframe era to be Howard Aiken / IBM's 1944 The Harvard Mark 1, which was mostly mechanical, consisted of ~750,000 separate parts, weighed roughly five tons, and utilized a system of punch cards to very slowly compute basic math. Over the coming decades, the underlying technology and functionality rapidly improved. For example, the vacuum-powered ABC computer eschewed physically moving parts to become the first electronic computer in 1941. The ENIAC became the first general-purpose electronic digital computer in 1945, allowing it to solve a large class of numerical problems. Other notable advances include: transistors functioned as electronic switches and replaced the vacuum tube in 1947, the

EDVAC used the binary system to improve efficiency and introduced storing programs to memory in 1949, and the UNIVAC became the first commercially available computer in 1951. Today, with large amounts of memory and processors to handle millions of transactions/large-scale batch computing, mainframe computers are in widespread use by corporate entities, powering the global finance industry and much of global commerce.

Personal Computers: As computers became smaller, cheaper, and easier to use, computing moved from off-line tasks like preparing punch cards to time-sharing systems to use by individual labs and research projects. These so-called minicomputers used integrated circuits and were the predecessors to what we now know as the personal computer, the movement of which started in earnest in 1971 after Intel released the first single-chip microprocessor. As the price of hardware fell drastically throughout the 70s, it became feasible for individuals to own their own computers. However, computers were seen as industrial-strength calculation machines confined to academics and hobbyists, and few at the time could understand why an individual would want one or what they would use it for. Moreover, personal computers required assembly and programming as the software industry did not yet exist. “Hobbyist” computers popped up like the 1973 Xerox Alto and the 1975 Altair 8800, but it wasn’t until 1977 when Apple unveiled the Apple II, the first computer that was fully assembled and offered for sale on the general market, that personal computing saw widespread commercial success. By the early 80s, Tandy (later known as Radio Shack), Commodore, and Apple were manufacturing popular computers, and IBM entered the fray with its IBM PC in 1981 and its first laptop in 1986. Now, with over one billion in use today, personal computers are ubiquitous and impact nearly every facet of our daily lives.

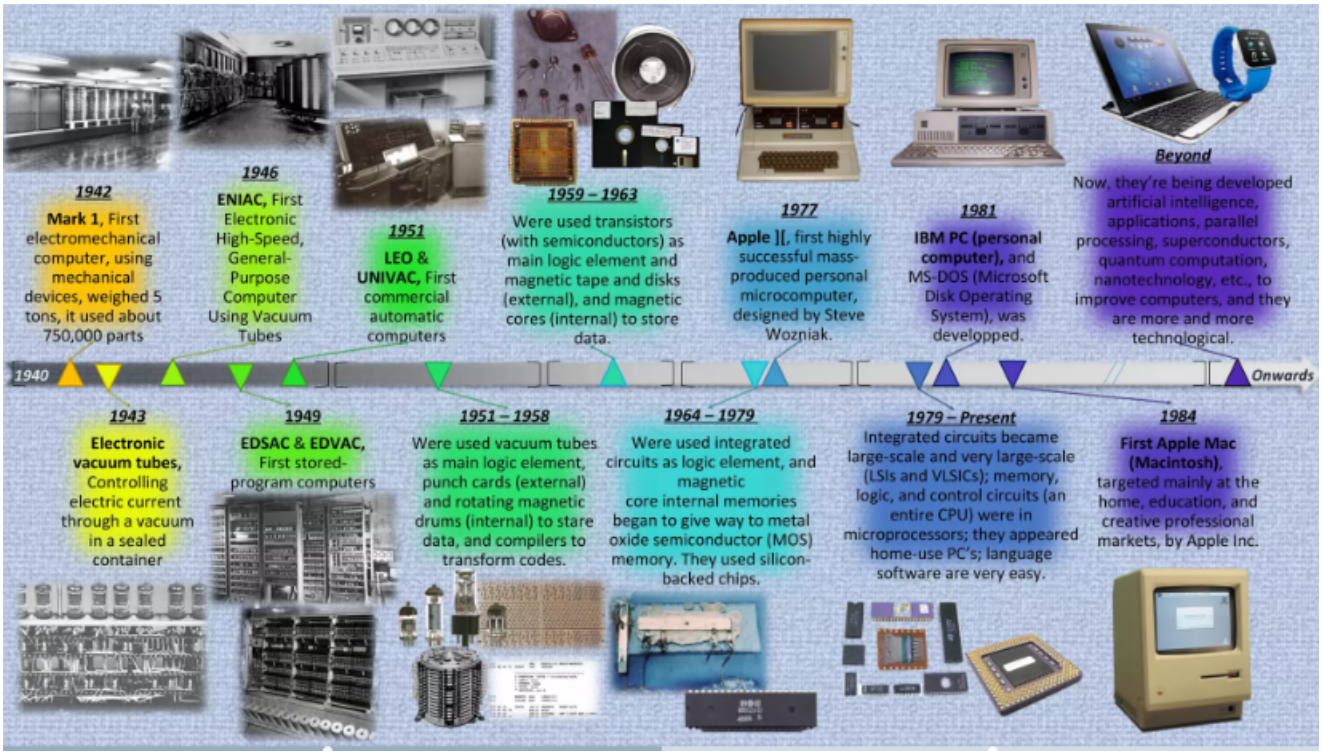
Public Computer: First conceived in 2013 by Vitalik Buterin and launched in mid-2015, Ethereum revolutionized computing by utilizing public blockchain technology to create a world settlement layer or decentralized state machine. No longer were nodes confined to one application, such as keeping a record of payments, but, starting with Ethereum, nodes on the network could process general-purpose code, adding programmability and arbitrary computation. Moreover, common smart contract standards and open-source code enabled applications to interact and build on each other, creating a composable programming environment. Anyone in the world with an internet-connected device can now permissionlessly interact with existing code or upload their own to the virtual machine, which the network executes in a trustless fashion. Creating such a virtual compute machine - owned by no one but used by all - enables the paradigms discussed above/not possible with existing computing constructs and effectively turns Ethereum and its smart contract blockchain peers into public computers.

One notable difference between this public computer and prior computing movements is that unlike in traditional technology where software is subordinate to hardware, this relationship is inverted, where in blockchain technology, software governs the hardware. Moreover, unlike traditional technology where the hardware may be changed by humans at any time, the code underlying the public computer is difficult to change, and when change does occur, it is done so in a manner that is community driven and credibly neutral. By having code run autonomously, exactly as written, the public computer is able to make commitments - for example, there only being one NFT - which brings about innumerable new possibilities. And, as the applications improve and evolve, they will inform the development of the underlying smart contract blockchains, which in turn will lead to improved applications, creating a virtuous flywheel along the lines of what we saw with the iPhone and its apps.

Lastly, there is reason to believe that the public computing era may develop faster than prior computing

movements. First, crypto/web3 is a software movement, so its speed is less reliant on the continued advancement of hardware. Second, crypto and web3 are predominantly open source, allowing developers to build on existing work, as well as composable, allowing new works to be built on top of instantiated code, making progress akin to compounding interest. Third, the technology comes with built-in incentives to reward users for participating in and contributing to the network. And fourth, community governance can determine how the infrastructure should change, allowing the technology to evolve much more flexibly compared to prior computing movements.

The History of Computing



Source: Carmen Bueno Inglesias, GSR

With an understanding of the evolution of the web and the computer, it appears as if blockchain technology and cryptocurrencies are at the heart of their next movements. Web3 will be the first instance of the web where users not only read and write data but also truly own digital items and communities. And unlike the corporate and personal computer, the public computer will offer open access for anyone to permissionlessly use or upload programs for the world to benefit, with both bringing about revolutionary capabilities and constructs.

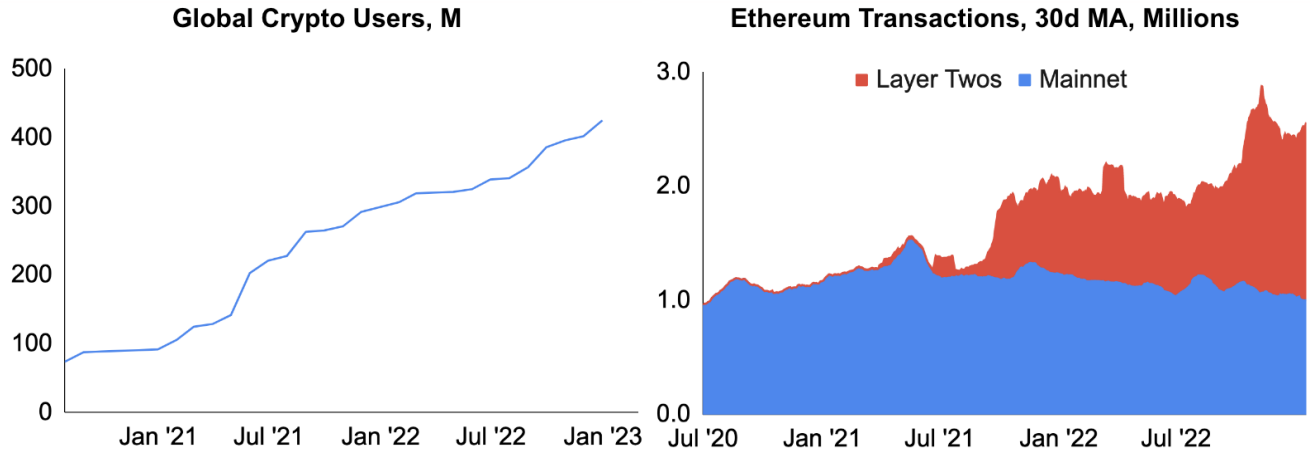
Long-Term Underlying Fundamentals

Another way to assess where crypto stands and where it may be headed is to examine its underlying fundamental trends, separating the cyclical (covered in the price section above) from the secular. Cyclical trends, as the name implies, tend to be shorter-term ups and downs, often revolving around economic cycles, while secular trends move in the same direction over long periods of time and are often driven by fundamental changes in consumer behavior, demographics, or technologies. As such, if

such long-term trends appear to be reversing, it's possible crypto may continue to contract and perhaps even eventually sputter out. However, if such trends remain strong, particularly in the wake of such large price declines, that would portend particularly well for the future of the technology. In what follows, we analyze various fundamental trends, including adoption and usage, technological development, industry talent, and capital inflows, all of which remain remarkably strong and make a case for secular expansion.

Adoption and usage remain robust, with the number of global crypto users up ~40% over the course of 2022 and the number of Ethereum wallets up 21% over the year. And while the number of transactions and active addresses on Ethereum mainnet have indeed fallen, they have hung in remarkably well relative to price, and we contend that much of the activity has moved to layer twos. In fact, the total number of transactions in the Ethereum ecosystem, which adds mainnet and layer two transaction counts together, increased over 30% from 4Q21 to 4Q22.

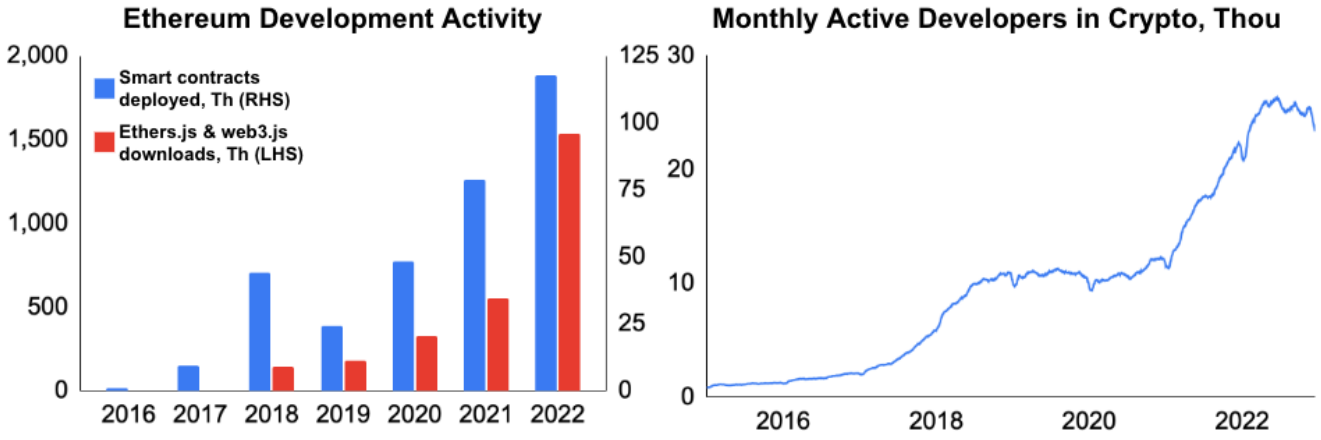
Crypto Usage & Activity



Source: Crypto.com, L2BEAT, GSR
Note: Total Ethereum ecosystem transactions simply add transaction counts from mainnet and layer twos together, so there is some double-counting as layer twos post data back to mainnet. We believe this to be modest, however. Moreover, L2BEAT employs a conservative definition of a layer two and excludes popular scaling solutions like Polygon POS.

In addition and despite the bear market, underlying technological development continues at a rapid pace. Ethereum, for example, had 48% more development-related events in its public GitHub repository during 4Q22 compared to 4Q21. Further, average weekly downloads of Ethers.js and Web3.js, essential tools for building web3 products, increased nearly 3x in 2022 from 2021, and the number of verified smart contracts increased by 50% over the prior year. Perhaps most importantly, the number of full-time crypto developers increased 8% year-over-year as of January 2023.

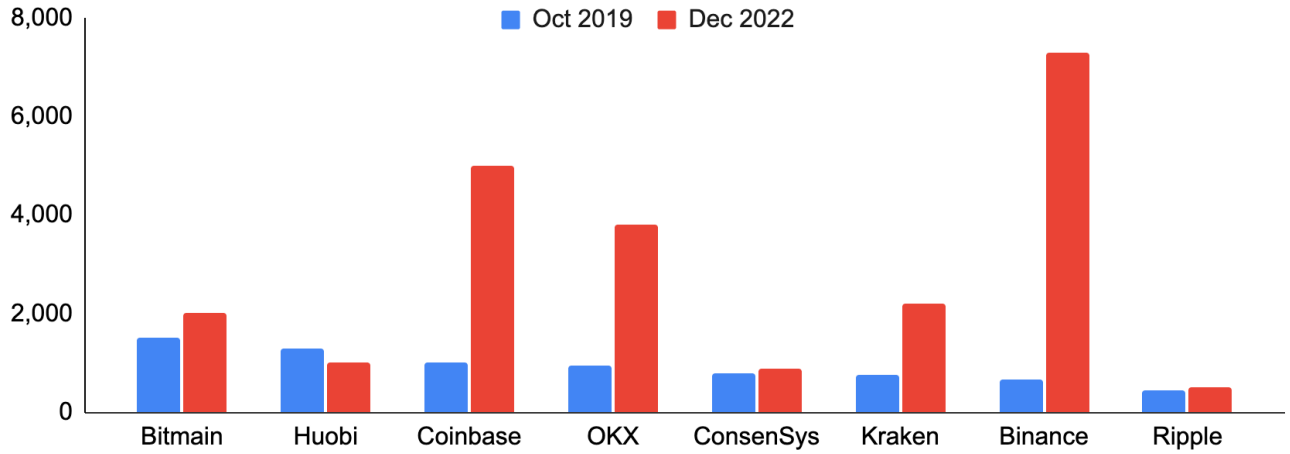
Web3 Development Activity



Source: Alchemy, Electric Capital, GSR
Note: Smart contracts deployed represent verified smart contracts used for the measurement of production applications. Ethers.js and web3.js downloads represent average weekly downloads.

Despite the frequent over-hiring of 2021 and more recent well-publicized layoffs, the influx of talent into the industry has been immense. Crypto job posts on LinkedIn, for example, increased 400% in 2021 over 2020. And The Block tallied industry employment to be ~82,000 employees at firms it tracks as of December 2022, up from ~18,000 in late 2019 for a nearly 5x increase in just three years. The estimated 9,500 layoffs in 2022 are certainly painful, and recent net employment gains in the space are likely negative, though some crypto companies continue to hire, such as Binance and Polygon, and employment levels remain leaps and bounds ahead of where they had been.

Employee Count at Select Digital Asset Companies, 2019 and 2022

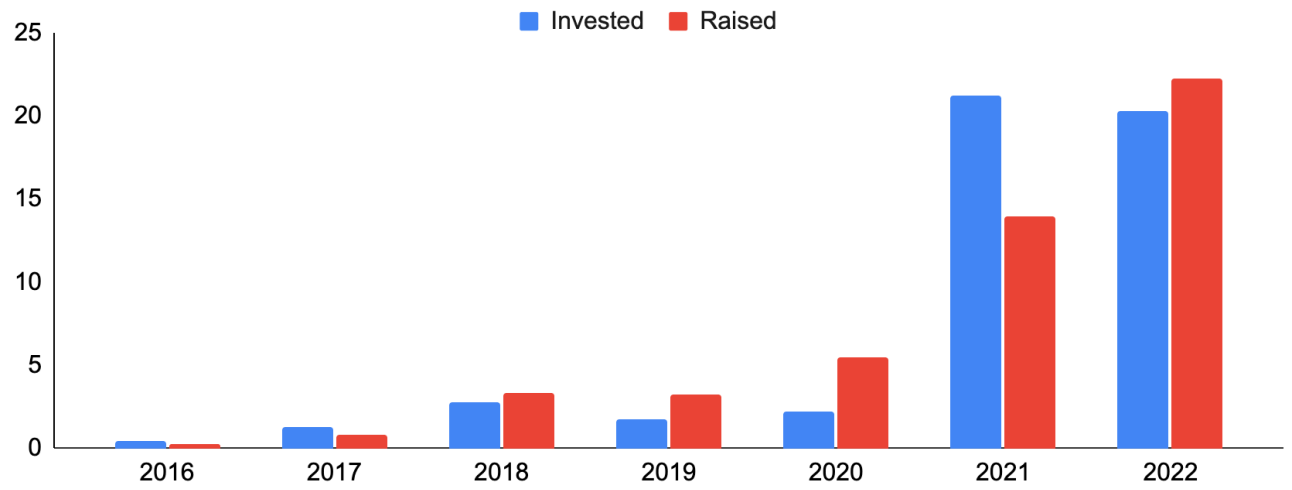


Source: The Block, GSR

Lastly, the space has attracted vast amounts of capital, which should fuel the industry for years to come. Venture investment, for example, totaled $20b in 2022, nearly matching 2021's record despite

lower valuations amidst the industry turmoil. And while the pace of investment fell significantly in the latter half of 2022, cumulative funds raised by venture capital firms to invest in blockchain/crypto skyrocketed over the last year, increasing 60% in 2022 to $22b and providing penty of dry powder for significant future investment. And beyond venture capital, corporate investment continues at a robust pace, with many of the largest global companies continuing to develop blockchain and crypto-related products and services, such as Google, Goldman Sachs, and Starbucks, just to name a few.

Total Crypto Venture Funds Invested & Raised, $b



Source: Pitchbook, GSR
Note: Total crypto venture funding for 2022 is through December 10, 2022. Crypto venture funds invested and raised may not be perfectly comparable.

With adoption and usage expanding by many measures, development continuing at a rapid pace, and a large influx of both talent and capital, crypto appears to be squarely in secular expansion.

Key Challenges

Another way to assess the current state of crypto and where it's headed is to examine its challenges and whether they may be overcome. If its main challenges are insurmountable, they will inhibit adoption and prevent crypto from truly competing with other technologies, but if they may be overcome, crypto is much more likely to reach its true potential. With that said, the biggest challenges for the industry, in our opinion, are a lack of regulation, weak security, a poor user experience, and low utility. These are immense challenges that will take years of hard work to overcome, and while we don't want to sound overly optimistic, we believe each will improve from here and help propel the space forward.

Regulation

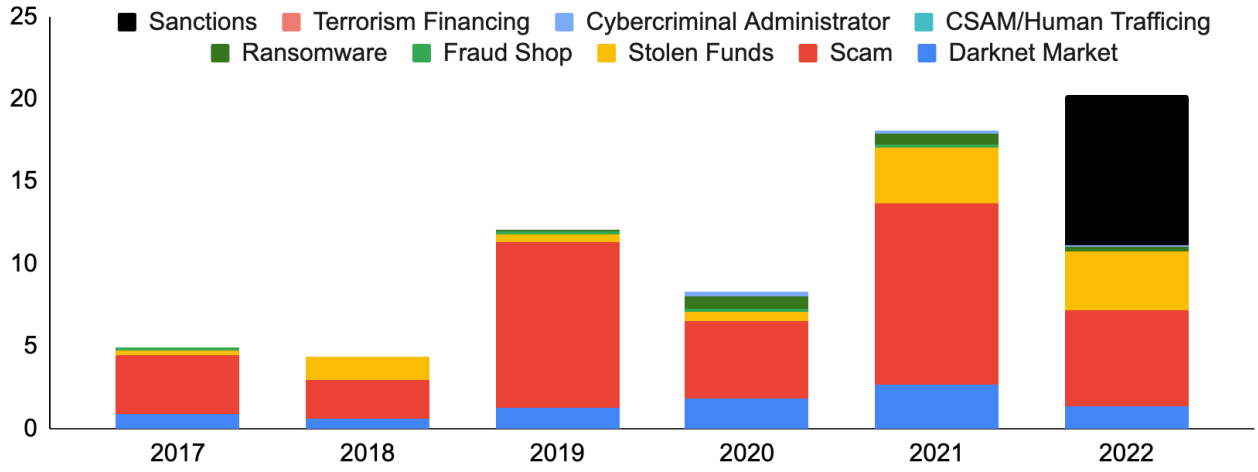
Despite the ability of blockchain technology to instantly instantiate trust, centralized crypto services require immense amounts of trust due to a lack of regulation, enabling bad behavior, increasing uncertainty, and disincentivizing participation and innovation. For example, when trading on an offshore, centralized exchange, users are outright trusting that the exchange is engaged in sound business

practices, is properly safeguarding its keys, and will return user assets when requested to do so - and there is often no way to recoup losses when issues arise given opaque jurisdictional legal recourse and unclear beneficial ownership. Fortunately, it appears that greater regulation and enforcement of centralized crypto services is on the horizon. The EU, for example, has largely finalized its cryptocurrency regulatory framework, the Markets in Crypto-Assets (MiCA), which the European Parliament will likely pass in April to give much-needed clarity to token issuers, trading platforms, and other crypto-asset service providers in the region. And though the US is further behind and unlikely to issue comprehensive crypto legislation anytime soon, increasing regulatory clarity and effective oversight is a priority for both the current administration and the various regulatory agencies, which should lead to improvement over time. Other jurisdictions such as the UAE and Singapore are also hard at work forming their own regulatory frameworks, often seeking to balance consumer protection and innovation. While there are many risks - globally coordinated regulations will take years, heavy-handed rules would stifle growth, and encroachment on decentralized ecosystems would hamper its benefits - it is the job of lawmakers and regulators to institute clear laws and regulations, which in our view are both a prerequisite and an enormous catalyst for ushering in the next wave of corporate and retail adoption.

Security

Outside of regulation, blockchain/crypto is rife with risks around security and safety. Smart contract risk, for example, introduces the potential for large-scale theft due to small coding errors, which is compounded by composability and incentivized by large attack targets. And as a bearer asset, participants are exposed to custody risk, where misplaced/compromised keys or poor access control can also lead to large losses. Scams are all too common, including phishing attacks, Ponzi schemes, and rug pulls, as are other forms of attack, such as oracle manipulations, flash loan attacks, and governance attacks. Add in layer one security concerns like reorgs, and Sybil/routing attacks, and crypto-specific financial risks such as exchange concentration/failures and stablecoin depeggings, and the cumulative risks are extremely high. While there is no magic bullet and it will take many years to reduce these risks to acceptable levels, efforts are already underway. Smart contract risk will improve from greater developer tooling, better smart contract testing techniques (egs. unit testing, static analysis, and formal verification), more secure programming languages, enhanced auditing models, new security and audit standards, rising bug bounties, and greater use of insurance. Custody risk will improve with simplified user experiences, smart contract wallets, new social recovery procedures, and advances in core technologies such as decentralized MPC solutions. Scams may lessen from identity verification, on-chain monitoring, attack simulations, and wallet tracing. Governance attacks can improve from more robust voting models like quadratic voting, improved economic modeling, and large holder token delegation. And L1 risk will decrease from Ethereum’s planned security improvements (like account abstraction, single secret leader elections, and single slot finality enabling quantum-resistant signature schemes, mitigating DDoS vectors, and reducing reorg risk, respectively) and shared security constructs (like Eigenlayer or Cosmos’ ATOM 2.0), among others. After the many risk events of 2022, we see clear regulations and improved security/safety as vital to the future of the technology, with many of the smartest in the industry working to improve on these key challenges.

Total Crypto Currency Value Received by Illicit Addresses, 2017 - 2022



Source: Chainalysis, GSR

User Interface / User Experience

Crypto is difficult and painful to use. From a convoluted user experience that requires downloading a browser extension, securing a seed phrase, on-ramping from centralized providers, and understanding blockchain/address basics all the way to slow speeds/high latency and high costs on Ethereum, crypto needs vast improvements in its UI/UX if the average person is going to use it. Fortunately, efforts are underway to abstract away the blockchain and move the user experience from that of web3 to web2. These include Ethereum's account abstraction plans for drastically improved wallet functionality and security, primitives/utilities like naming and notification services (e.g., ENS, EPNS/Push), and a general focus on increased mobile accessibility, reduced latency, improved privacy and interoperability, and further integration with traditional financial services. Moreover, significant progress has been made on scaling, with layer two solutions and alternative layer one blockchains offering near-instant and near-free transactions, as well as with Ethereum's thoughtful scaling plans enabling transaction processing that may rival that of Visa and Mastercard. UI/UX will have reached its destination when an Uber driver clicks the "hedge gas costs" button within his or her Uber app, which, unbeknownst to the driver, utilizes a decentralized exchange on the back end to lock in fuel prices with just one click. This won't happen overnight, but crypto is becoming accessible to all.

Utility

Tokens are one of crypto's key innovations, coordinating and incentivizing behavior, rewarding value contribution, and enabling exchange. Unfortunately, however, they may be used for financial incentive schemes that can collapse just as quickly as they appeared like with liquidity mining, or worse, utilize Ponzinomics that are especially dangerous when obfuscated behind layers/complexity, such as some play-to-earn games or bond-based decentralized reserve currencies. However, a renewed focus on utility over financialization is yielding results. For example, DEXs are moving away from short-term incentives to attract liquidity in favor of providing increased utility elsewhere, such as with GMX's sleek user experience with no price impact trades or DeFiLlama DEX aggregator's free data and analytics. Blockchain-based games are prioritizing making games users actually want to play before focusing

more on the blockchain-based components. And decentralized reserve currencies are concentrating on token usage via greater access and liquidity as well as tangible services like protocol-owned liquidity over eye-popping but short-lived incentives. Venture capital firms too are becoming much more discerning and hyper-focused on tangible use cases and product market fit in lieu of rewarding cool experiments. While the financially incentivized experimental days are over, many are hard at work building applications with real use cases and significant utility.

Overall, it will be a long road, and the industry's challenges are formidable. A lack of regulation, poor security and safety, poor UI/UX, and often low utility currently plague the space. However, efforts are underway to improve upon each, and given their importance, an entire industry is motivated to figure it out for all involved.

Areas of Particular Hope

Another way to understand what blockchain/crypto may become is to look at areas of particular hope, as these may demonstrate tangible use cases and benefits large enough to onboard large swaths of the population. We see several innovative areas of blockchain/crypto with this potential, including zero-knowledge proofs, decentralized identity, modular blockchains, and decentralized infrastructure networks that, together with the more well-known areas of the space like payments, DeFi, NFTs, DAOs, and web3 are capable of ushering in humanity-changing paradigms.

Zero-Knowledge Proofs

With its main use cases in privacy and scaling, and applications ranging from finance to identity, compliance, governance, healthcare, gaming and more, zero-knowledge proofs (ZKPs) allow for one to prove that a statement is true without revealing any other information. Long in the realm of the theoretical, ZKPs are quickly moving to the practical and are improving upon key areas like prover time, proof size, verification time, and the trusted setup. ZKPs utilize arithmetic circuits to prove the validity of statements, may be interactive or non-interactive, and most often take the form of zk-SNARKs in crypto. ZKPs enhance privacy by allowing one to hide transaction information, anonymously pool and analyze data, and minimize the amount of information shared, for example, by allowing one to prove citizenship without providing a tax ID or passport, prove blood type to a health insurer without revealing other health details, prove trade compliance to the government without sharing transaction data, or prove that net worth and income qualify for a loan without sharing personal financial information. Crypto mixer Tornado Cash is one live example, where users may deposit Ethereum and ERC-20 tokens to its smart contract, later withdrawing tokens from the contract after zk-proving they were a depositor without revealing any other information, breaking the link between token origin and destination to add anonymity to an otherwise public blockchain. On the scalability side, ZKPs enable verifiable outsourced computation, allowing layer two networks to perform off-chain computation while later submitting proposed state changes as well as zero-knowledge validity proofs to prove the correctness of the proposed changes back to the main chain, improving speed while inheriting the security of the underlying chain. Including similar technologies like multi-party computation (MPC) and fully homomorphic encryption (FHE), we are on the verge of cloud-scale, verifiable, outsourced computation

(a la zkEVM), open third-party analytics on anonymized data (a la ZKML), enhanced trust and privacy at the same time (with decentralized identity), and even new paradigms in the blockchains themselves (full nodes may no longer need to process all transactions).

Decentralized Identity

With the average internet user having 100 passwords, identity fraud leading to $52b in losses in 2021 in the US alone, and 1.1b people globally unable to prove their identity to access basic rights and services, the current model of identity is broken. Identity on the internet has moved from a centralized model where users create accounts with individual websites to a federated one where users sign in through Google and Facebook, exchanging privacy for convenience and security. However, identity is gradually moving towards a new decentralized paradigm, known as self-sovereign identity (SSI) or decentralized identity, where users own and control their personally identifiable information (PII) and data without the need for centralized parties. Decentralized identity uses decentralized identifiers (DIDs) - globally unique, verifiable, private key-controlled identifiers for people, entities, and even actions and ideas - and verifiable credentials (VCs) - tamper-resistant, instantly-verifiable digital credentials provided by issuers and stored by holders in identity wallets. Combined, DIDs and VCs allow holders to prove ownership of the DID and assert claims that can be cryptographically authenticated by verifiers. Decentralized identity gives way to improved experiences (e.g., sign in with your wallet, achieve gated access, and bring your own data for one-click checkout/instant financial services access/portable social graphs), greater remuneration and reputational benefits (receive payment for sharing data or viewing ads, take out an undercollateralized loan), enhanced privacy (selective disclose like proving that you're over 21 without sharing your birthday or age), and reduced risks (tamper/ counterfeit-proof credentials residing in cryptographically-secured wallets rather than large, hackable databases spread across numerous institutions). Moreover, decentralized identity decouples data from the application layer, allowing apps to compete on their primary services rather than on data collection, leveling the playing field for new entrants and enhancing competition for the benefit of users. And with use cases ranging from identity verification to compliance, access control, Sybil resistance, governance, employee management, medical records, supply chains, and many more, decentralized identity may one day impact every facet of our digital lives.

Modular Blockchains

Vitalik Buterin coined the notion of The Blockchain Trilemma, arguing that it is impossible for a blockchain to be decentralized, secure, and scalable at the same time. Increasing block size, for example, would improve speed but would lead to a larger blockchain, making it prohibitive for some nodes to keep a full copy, reducing decentralization. However, whereas traditional monolithic blockchains performed all four functions of a blockchain in execution, consensus, settlement, and data availability, a new breed of protocols is separating out and optimizing each function. Such modular protocols liken their efforts to what Henry Ford did with the Model T and specialization, allowing each component of the modular stack to be optimized and come together for a more decentralized, secure, and faster blockchain. Additionally, the underlying technology of monolithic chains continues to increase in complexity, and modularizing can ease blockchain fixes/upgrades. The most famous modular blockchain is Ethereum, which has chosen to improve scalability by outsourcing execution to layer two networks. While Ethereum can still operate as a monolith, it is moving towards performing consensus,

settlement, and data availability while utilizing layer two scaling solutions for off-chain execution. Celestia is another example, which provides transaction ordering and data availability using data availability sampling and erasure encoding to prove that sufficient data was made available to replicate the blockchain's state, and allows other modular components to plug into Celestia's network to quickly spin up interoperable, customizable, highly performant blockchains. Others include Fuel (a modular execution layer), Tezos (a layer one with an enshrined rollup), and Polygon Avail and EigenDA (data availability layers). To be sure, modular blockchains have several challenges to overcome to truly achieve their vision, such as L2 centralization with their sequencers as well as fragmented liquidity, as execution layers are mostly non-interoperable with each other. However, modular blockchains just might represent our best hope to achieve the security, speed, and decentralization all at once to finally solve The Blockchain Trilemma and enable mass adoption.

Decentralized Hardware Networks

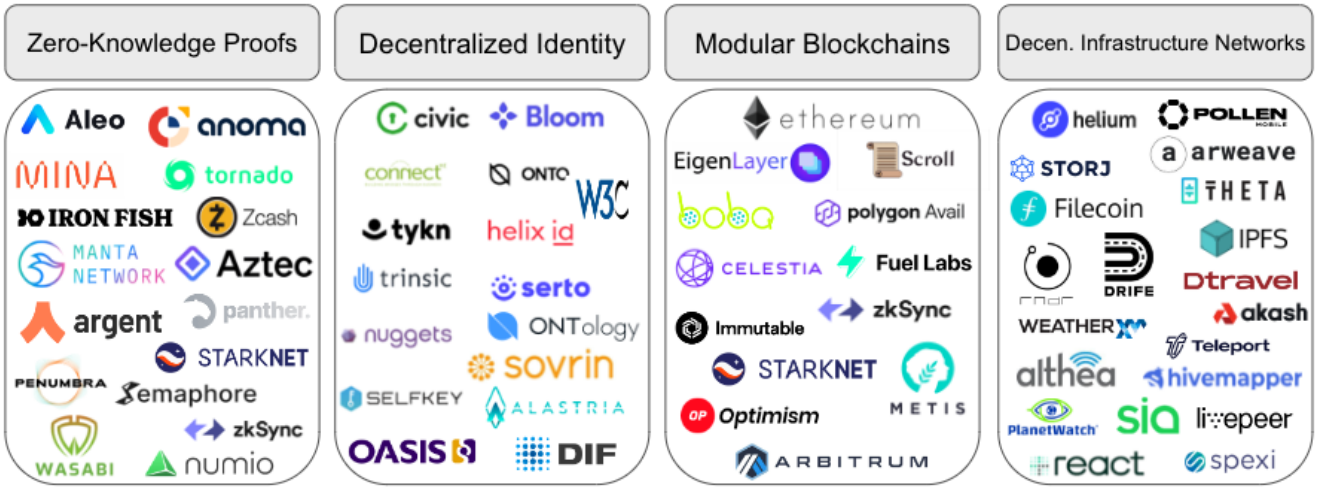
Blockchain technology innately enables the creation of P2P sharing networks and marketplaces that efficiently incentivize, allocate, and transfer resources between peers. Such resources may be service-based, such as tokenized data indexing (The Graph), tokenized KYC (Shyft Network), or tokenized jobs markets (Human Protocol), or they may be related to physical infrastructure, which is particularly powerful given the ability to challenge large, centralized oligopolies who are often otherwise untouchable given the billions in infrastructure investment required to compete. Such decentralized infrastructure networks bootstrap their hardware systems using cryptoeconomics, incentivizing users to purchase and operate devices on the network with protocol tokens or enabling the use of already-existing idle resources in exchange for payment. Such token-incentivized physical infrastructure networks (TIPIN) were pioneered by Helium Network, which awarded protocol tokens to individuals who purchased and operated nodes providing connectivity to IoT sensor devices, effectively bootstrapping the world's largest LoRaWAN network (and one largely owned and operated by the community). Other protocols such as Filecoin and Arweave allow users to rent or purchase unused hard drive space on others' machines in exchange for FIL or AR tokens, putting excess storage space to use while also increasing data persistence and censorship resistance as files are stored on multiple machines. Decentralized infrastructure networks are being deployed across vast areas of hardware, including 5G, broadband, compute, mapping, ridesharing, accommodations, energy, and weather sensors. All in, with its ability to incentivize hardware development or use, decentralized infrastructure networks may soon challenge the tech and infrastructure giants who rule the world.

Existing Areas - Payments, DeFi, NFTs, DAOs, and Web3

We'd be remiss not to mention the more well-known areas of crypto, including payments, DeFi, NFTs, DAOs, and web3, each of which have the ability to change everyday life as we know it. Blockchain-based payments, for example, bypass antiquated traditional rails (and intermediaries) to enable near-free and instant permissionless value exchange that can be used for remittances, micropayments, and trade finance, among others. DeFi, a form of finance that uses blockchain technology, smart contracts, and decentralized applications to offer typical financial services in a transparent and open way, has the potential to replace the existing financial services industry to offer lower costs, faster speeds, permissionless access, and improved transparency. As blockchain-based digital representations of ownership, NFTs enable ownership in the digital realm that, with the benefits

of programmability and composability, will enable new constructs around content, ownership, value, and exchange. Decentralized autonomous organizations (DAOs) enable self-organized online communities following smart contract-based rules and community governance to enable bottom-up decision-making, organization around shared goals, borderless collaboration, and community-driven ownership and reward based on true merit. And using blockchain technology and tokens to enable ownership, identity, value exchange, and coordination/incentivization, web3 is the next iteration of the web, built, owned, and operated by users to bring all these concepts together to enable digital ownership, digital identities, wholly native payments, and community governance.

Areas at the Forefront of Crypto Innovation



Source: GSR

All in, these cutting-edge areas demonstrate tangible use cases and benefits with the potential to onboard large swaths of the population. From zero-knowledge proofs to decentralized identity, modular blockchains, and decentralized infrastructure networks, the opportunities to change the world are enormous.

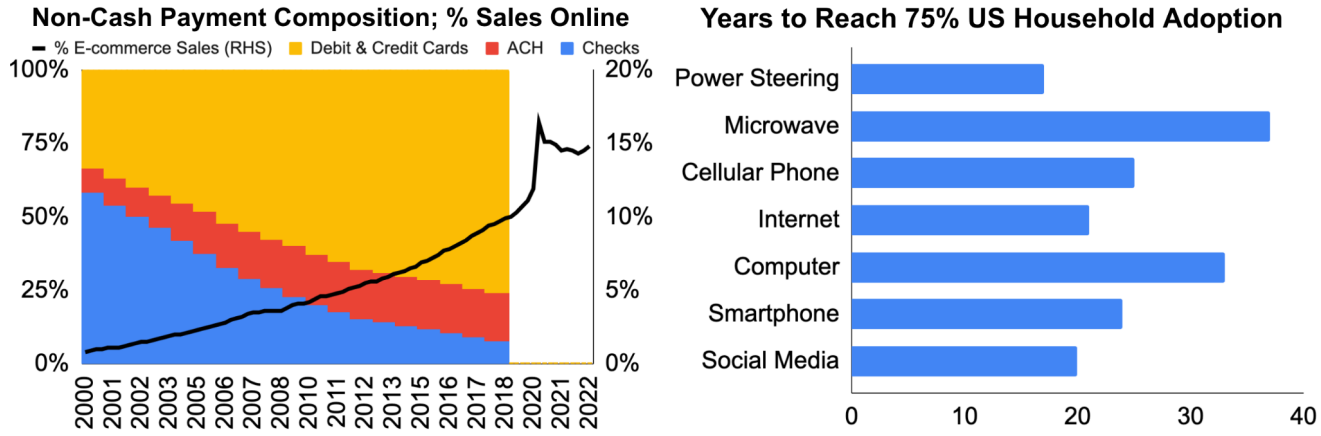
Conclusion

The numerous risk events of the past year and precipitous drop in token prices have put cryptocurrency shortcomings on full display and have pushed even the most ardent supporters towards despondency and pessimism. Formerly revered firms no longer exist, once-respected industry titans will soon wither in jail, and billions of dollars have been destroyed. It will take years to fully recover from these events.

That said, if history is any guide, it was always to be a long path towards changing the world, as shifts in consumer behavior and technology adoption take decades to play out. For example, many consumers still use checks rather than credit and debit cards or buy items in physical stores rather than online. It similarly takes years for new technologies to garner mass adoption and resemble their final form, such as with the microwave taking 37 years from its invention until it achieved widespread household use and the internet taking 22 years from the time it was first made commercially available

until 75% of US households had access. The good news is that changes in consumer behavior and technology adoption, though slow, are incredibly steady. And with crypto just seven years from the launch of Ethereum, it is clearly both very early and well on its way.

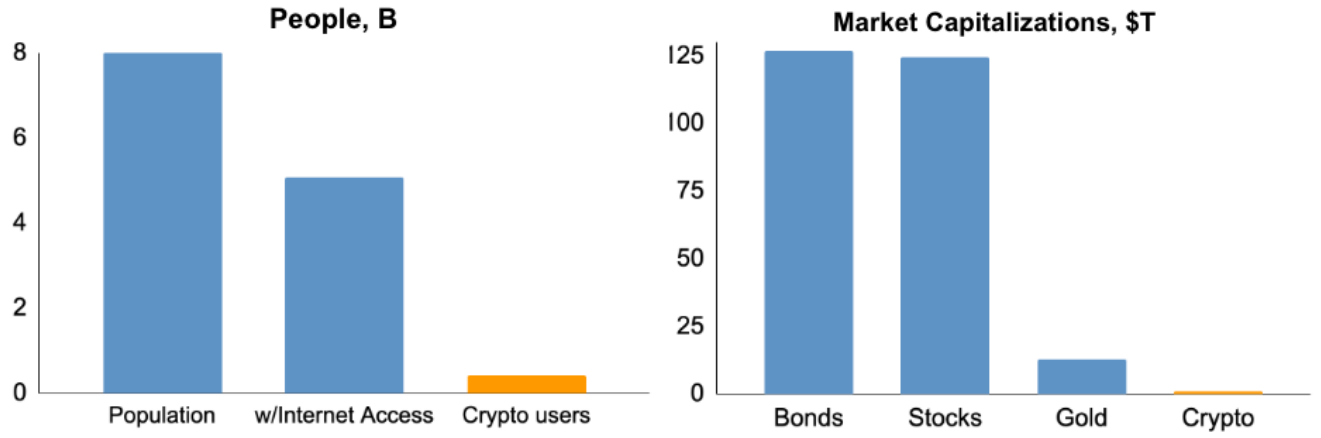
Changes in Consumer Behavior & Household Adoption of New Technologies



Source: US Census Bureau, Federal Reserve, Our World in Data, GSR
Note: There is considerable debate as to when many of these technologies were invented and as such, we use our best judgment to pick the year each technology first became commercially available. The first power steering system fitted to a production car was to the Chrysler Imperial in 1951; Raytheon licensed its patents for a home use microwave oven that was introduced by Tappan in 1955; DynaTAC 8000x was the first commercially available handheld mobile phone in 1983; Limited private connections to parts of the internet by officially commercial entities emerged in several American cities by late 1989; The Simon Personal Communicator by BellSouth was the first smartphone marketed to consumers in 1994; and, Six Degrees is the generally accepted first social media site and was founded in 1997.

With the potential to impact how we work and earn a living, socialize and interact with others, acquire goods and services, and many more, the opportunity is massive. The 425m crypto users today represent just 5% of the global population and just 8% of those with internet access, a far cry from the potential upside scenario of ubiquity. And from a financial perspective, the total cryptocurrency market cap represents just 0.8% that of both equities and bonds, providing immense potential that includes the possible tokenization of the other asset classes.

The Crypto Opportunity



Source: SIFA, Gold.org, CoinMarketCap, Worldometers.info, Datareportal.com, Crypto.com, GSR

While the severe decline in prices has led to draconian sentiment, we contend that such volatile price action is normal and expected, given the nascency of the technology, and that it was mainly driven by sentiment and the macro environment rather than a change in crypto's underlying fundamentals or what the sector may one day become. And with significantly greater upside, the smart money is doubling down.

Near-term, we are likely in for a long winter. But the bad actors have been exposed, the fast money has been flushed, and now only true believers and builders remain. Prices over the short-term will likely move with the macro backdrop, briefly deviating as the occasional crypto-specific catalyst or risk comes to fruition. But over the long-term, prices will move with the fundamentals, and crypto fundamentals remain strong.

Look no further than its use cases and benefits, which supplant those of existing technologies and include the removal of intermediaries, the democratization of value exchange, and new paradigms around governance, ownership, and business models. And thanks to these use cases and benefits, we are on the verge of the next iteration of the web, one built, owned, and operated by its users rather than big tech, as well as the next iteration of the computer, a decentralized, trustless virtual computer owned by no one but used by all. Underlying fundamentals such as adoption/usage, development, and inflows of both talent and capital remain strong and place us squarely within a larger secular upswing. And while challenges around regulation, safety, UI/UX, and utility are enormous, efforts are underway to improve upon them, suggesting each will progress from here. Lastly, cutting edge areas of the technology such as zero-knowledge proofs, decentralized identity, modular blockchains, and decentralized infrastructure networks offer additional opportunities to change the world. So despite the atrocious year that 2022 was, the future of crypto has never looked so bright. In short, we still believe.

Editor's Note: The views expressed in this report are solely the author's and do not necessarily represent those of GSR.

About GSR

GSR has over a decade of deep crypto market expertise as a market maker, ecosystem partner, asset manager, and active, multi-stage investor. GSR sources and provides spot and non-linear liquidity in digital assets for token issuers, institutional investors, miners, and leading cryptocurrency exchanges. GSR employs over 250 people around the globe, and its trading technology is connected to 60 trading venues, including the world's leading DEXs. We have a culture of approaching complex problems with tenacity and imagination. We build long-term relationships by offering exceptional service, expertise and trading capabilities tailored to the specific needs of our clients.

Find out more at www.gsr.io.

Follow GSR for more content: Twitter | Telegram | LinkedIn

Required Disclosures

This material is provided by GSR (the "Firm") solely for informational purposes, is intended only for sophisticated, institutional investors and does not constitute an offer or commitment, a solicitation of an offer or commitment, or any advice or recommendation, to enter into or conclude any transaction (whether on the terms shown or otherwise), or to provide investment services in any state or country where such an offer or solicitation or provision would be illegal. The Firm is not and does not act as an advisor or fiduciary in providing this material.

This material is not a research report, and not subject to any of the independence and disclosure standards applicable to research reports prepared pursuant to FINRA or CFTC research rules. This material is not independent of the Firm's proprietary interests, which may conflict with the interests of any counterparty of the Firm. The Firm trades instruments discussed in this material for its own account, may trade contrary to the views expressed in this material, and may have positions in other related instruments.

Information contained herein is based on sources considered to be reliable, but is not guaranteed to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made by the author(s) as of the date of publication, and are subject to change without notice. Trading and investing in digital assets involves significant risks including price volatility and illiquidity and may not be suitable for all investors. The Firm is not liable whatsoever for any direct or consequential loss arising from the use of this material. Copyright of this material belongs to GSR. Neither this material nor any copy thereof may be taken, reproduced or redistributed, directly or indirectly, without prior written permission of GSR.