Blockchain technology and Web3 have bled into mainstream consciousness by way of incendiary headlines surrounding the speculation on and valuation of cryptocurrencies and the dawn of the Metaverse. Below, we ground ourselves and you in the current reality and the promise of Web3 and blockchain technologies. This is intended as an initial primer for those less familiar with Blockchain and Web3. For those that have already gone deep on Web3 developments, we would welcome further conversation.

Overview

Web3 is an evolution from the *read-write* era of Web 2.0 to a new period of *read-write-own* in which certain classes of digital assets endowed with rights can be uniquely and distinctly owned without a central organization capable of seizing these assets. This form of off-platform ownership is powered by blockchains like Bitcoin and Ethereum rather than platform companies like Facebook or Amazon. Blockchains themselves are forms of distributed computers which can only operate in well-defined ways, and which are not controlled directly by a central party – as a result users can own digital assets on blockchains with a relatively high sense of security.

Building applications directly on top of blockchains have historically ranged from near-impossible (in the case of Bitcoin) to prohibitively expensive (in the case of Ethereum) but today more focused, energy efficient blockchains (like Solana and Polygon) have advanced to a point that the infrastructure now exists to begin building useful Web3 applications that could not exist in the context of the platform-based Web 2.0 space. For example, despite the distracting valuations and personalities associated with NFTs today, the technology underlying NFTs and similar digital assets likely enables novel and broad-based applications.

Despite the potential of Web3 to usher in a new era of interconnectivity, for reasons we hope will be clear as you read, ***we will not be recommending investments in specific cryptocurrencies***. The space is highly complex and one in which nuances matter tremendously; instead, this primer is intended to be a thoughtful zero-to-one introduction to how to engage with the Web3 ecosystem.

The topics covered in this paper are:

1. A historical description of the internet as it undergoes sea changes that unlock new forms of applications to ever broader audiences
2. An introduction to the mechanics of the blockchain and how the structure of a blockchain enables new use cases.
3. The concept of a blockchain's monetary policy and how it can potentially lead to a non-zero value for cryptocurrencies.
4. The concept of smart contracts and how these unlock new applications.
5. NFTs and how the current hype around JPEG valuations obfuscates a useful class of technology.

From Web1 to Web 2.0 to Web3

Web1 was the *read* period, an early stage of the internet prior to the turn of the millennium when webpages were viewable but not interactive. This included the early blogs in which a moderately tech savvy person was able to independently develop and manage a webpage.

Web2 (at the time styled Web 2.0) is the *read-write* period beginning in the early 2000's and lasting through today when webpages became interactive, allowing users to upload and download data programmatically to centralized databases through websites. Web development became more difficult for single users given this added complexity. The shift from Web1 to Web2 lowered the time and effort required to do interesting things online to near zero and provided services that invited many more people online (i.e. Facebook, Netflix, and Google Maps etc.) while also consolidating activity on privately owned platforms able to continuously spend to keep their services competitive.

Web3 refers to a new *read-write-own* period. It is nascent today but offers compelling features and solutions beyond what can be built in Web2 frameworks. Whereas the storage and compute infrastructure of Web1 and Web2 were usually owned or leased from a platform, Web3 applications are built on top of a distributed infrastructure generally constructed around blockchains. Today those involved in developing Web3 are often in the business of hashing out what the best infrastructure should look like rather than building cash flowing business on top of the infrastructure. As a result, popular knowledge of Web3 is limited and the press spends more time discussing movements in cryptocurrency prices than any specific applications that might come from this next generation of internet platform.

Glossary

In much the same way it would be difficult to discuss Web 2.0 without a sense of what a social network is, it is worth defining some terminology prior to launching into a discussion of Web3.

Block: A collection of transactions data added to a blockchain in order to update its state. Data added is grouped into discrete blocks to be added to the chain. A block is a group of records of information that need to be or are being validated. A block also holds information about other blocks connecting them; thus, creating a chain. Once a block is done being validated those transaction records become immutable and are added to the ledger.

Blockchain: a data structure stored across many computers, agreed upon and updated synchronously by the addition of blocks. A blockchain must exist in a state such that all prior states can be calculated from the current state. As such, data can only be added and never deleted.

Coin or Token: A digital asset owned by an account on the blockchain which can be exchanged via a transaction to another account, for example to pay a fee.

Consensus rules: the set of rules that that determine the validity or applicability of data added to the blockchain. A common rule is that an account cannot send more tokens than the account currently holds; another is that accounts can only send tokens that there is a record of the account coming into possession of. Another would be that you have the records and other blocks on the chain reflect that you own the current coins you are trying to send.

Decentralization: a system in which data is publicly distributed in a peer-to-peer network rather than being maintained and controlled by a predetermined central entity. Often interchangeable with distributed.

DeFi: decentralized finance; the concept that blockchain ecosystems can fulfill some needs traditionally met by the banking sector, including payments, saving, borrowing and lending denominated either in floating cryptocurrencies or cryptocurrencies pegged to the US dollar known as stablecoins.

Mining: the competition of intentionally difficult tasks (often complex calculations) associated with maintaining or adding to a blockchain, generally associated with proof-of-work blockchains. Mining activity is typically compensated with tokens.

Node: a computer containing the entire blockchain and allowing public access to the chain. Depending on the specific blockchain, the minimum requirements to act as a node could be as little as a cheap laptop or as much as a dedicated server. Nodes are what blockchains are distributed across and what allow for decentralization.

Proof of Stake: a consensus mechanism used to validate a blockchain. Miners stake a certain amount of crypto currency making them eligible to be chosen to validate a block. If the user acts in bad faith or fails to validate due to external factors, their crypto can be slashed or taken away from them either in part or whole. This promotes reliable stakes. Since miners are not competing against each other to solve the complex equations, this requires far less computational power which translates to less electricity usage than Proof of Work.

Proof of Work: a consensus mechanism used to maintain a blockchain and a method by which to classify categories of blockchains. In a proof of work blockchain, users can choose to compete to solve complex computational problems to receive token rewards, a practice called 'mining'. A small piece of the completion of these calculations involves the work necessary for maintaining and adding to the blockchain. The proof of work mechanism results in very large amounts of energy usage.

Smart contracts: programs that are set to execute given a current state is reached outlined by predetermined conditions. Smart contracts are written directly into the blockchain and are thus public and immutable.

Staking: The locking-up of tokens in order to receive a share of fees on a proof of stake blockchain with the amount of tokens stakes being proportional to the share of fees received. Staking reduces the freely tradable number of tokens and is a way to push up the value of the tokens. It is typically associated with proof-of-stake blockchains.

Transaction: the data to be added to the blockchain. A simple transaction would be the moving of tokens from one account to another, but simple transactions can be assembled into more complex smart contracts. Often abbreviated txn.

Wallet: a front-end application that allows the account's owner to more easily interface with Web3 applications often through public and private "keys" or unique multi-character identifiers.

What is a blockchain and what can it do?

The blockchain is a distributed ledger, public and programmatically agreed upon by the users of the chain that can be extended by the addition of agreed upon "blocks." The blockchain lives on computers and phones of those who participate in sponsoring the chain (the "miners"). Those in charge of maintaining the public record of the chain and agreeing upon new blocks are compensated for doing so in the form of tokens or coins. The value of coins is a function of the demand for use of the chain and the scarcity of new blocks; when an agent would like to transact on the blockchain, they must pay in the form of coin – known as a "gas fee" - to those maintaining the agreed upon record. If the blockchain provides a desirable service, the demand for the coin to pay for the service should result in a non-zero price for the coin. This provides incentives to those maintaining and adding to the chain to continue to do so.

Each blockchain can be distinguished based on two core elements:

1.) How the blockchain is maintained
2.) What is being added to the chain

Further, while numerous blockchains have been created and more are being established every day, they all exist within what's called the *Blockchain Trilemma*. Blockchains are inherently forced to make tradeoffs between *Decentralization, Scalability,* and *Security* but no chain can be efficient at all three. New blockchains have been created that exist in different spots within this so-called *Trilemma* to optimize performance toward different use cases.

So far, we have considered a very general depiction of a blockchain, but let's apply this framework to the most popular blockchains today.

Bitcoin

As the first blockchain of note, Bitcoin maps neatly to the description above. It is relatively secure, and decentralized, but not particularly scalable.

Bitcoin is known as a proof-of-work chain meaning that the maintenance and validation of the chain is completed through the solving of difficult calculations by distributed computers on the network, a process referred to as mining. The agents, in this case powerful computers, solving the calculations are referred to as miners who are rewarded with an amount of bitcoin for helping to solve the calculations. The amount of bitcoin rewarded to miners per calculation completed declines asymptotically over time. The data that miners are facilitating adding to the bitcoin blockchain is exclusively bitcoin transactions. As a result, the bitcoin blockchain is nothing more than a decentralized, indelible ledger of bitcoin transactions with a maximum number of 21 million bitcoins that will ever exist, most of which have already been mined. While this has use cases, including cross boarder secure, verifiable coin transfers outside of the typical monetary system, those use cases are limited.

Ethereum

Ethereum is highly decentralized and relatively secure but like Bitcoin, it is limited in its scalability. Also like bitcoin, Ethereum is currently a proof-of-work blockchain[1] in which the maintenance and validation of the chain is managed by miners completing calculations. That said, the Ethereum chain differs from the Bitcoin chain in important ways: unlike Bitcoin, it is relatively open ended as to what can be added to the chain. In addition to adding transactions to the chain, functional subroutines can be added to the block chain that operate similarly to computer applications that can perform basic tasks. Today, the task of executing these programs is endowed with a high degree of difficulty. Miners provide the computational power to execute these applications but because of the proof-of-work structure of the blockchain, they are implicitly executing these programs through a layer of complex calculations which results in massive need for additional computational power to execute even simple programs. Thus, the chain is slow and expensive to use but relatively flexible as to what it can be used for.

For example, on top of Ethereum, a music streaming application could be built to securitize the platform's royalty streams. An artist could, for example, upload a song to the platform and then embed the rights to the future fees paid by the platform for streaming the song. These tokens could then be sold, not unlike the selling of music royalties. The benefit of building this system on top of the Ethereum blockchain is that the system is trustless, i.e., that fees are paid to the accounts token holders mechanically not by a centralized party but rather by the blockchain itself.

[1] *While today Ethereum is a proof of work blockchain, on the horizon for several years have been plans to upgrade the Ethereum protocol to proof of stake like Solana described below.*

Upgrading a blockchain: *While blockchain histories are indelible, the protocol for adding new data to the chain is not and Ethereum regularly deploys marginal upgrades to the system, mostly focused on improving network speeds or general network usability. Because Ethereum is a decentralized project, upgrades are not executed unilaterally but rather a result of a public process in which improvement proposals are vetted and coordinated to eventually become consensus among the managers of the Ethereum nodes. When in the case that an upgrade is not fully consensus, but a significant portion of nodes implement the upgrade anyway, the chain undergoes a fork in which nodes are attempting to add to the chain under two different protocols which results in two new forward chains that share a history. The forking process results in two distinct tokens, typically one of which (generally the more likely heterodox token) loses its value quickly as the community using the token settles on a favorite. This was the case for Bitcoin Cash, which was the new token created by a controversial upgrade to Bitcoin block sizes. Many in the Bitcoin community rejected the upgrade in block sizes in order to keep the Bitcoin network able to be run on smaller nodes and thus more decentralized and as a result the upgrade created a new chain.*

Solana

Solana is less secure and decentralized than Bitcoin or Ethereum but highly scalable. Unlike Bitcoin and Ethereum, Solana is a proof-of-stake blockchain which does not require miners completing difficult calculations to maintain and add to the chain. Instead, Solana uses validators who add to the chain via a consensus mechanism. As a result, Solana is less robust against attacks[2] but massively cheaper and faster computationally than the current Ethereum system. This is leading to much faster, much cheaper execution of "smart contracts." Like with Ethereum, validators are paid through both an issuance of tokens from the chain and through *gas fees* paid by users. Since there is no competition on the allocation of compute power however, validators compete based on their stake of tokens. Solana uses a range of mechanisms to balance security with incentives but most simply put for each block a random validator is selected as the lead validator for the block. While all validators independently validate all transactions, the lead validator is the individual validator in charge of ordering the transactions within the block, after which all other validators vote on the ordering being true. In the case of a bad-actor lead validator, the lead validator mechanistically cannot add transactions violating the consensus rules but could drop or 'censor' certain transactions. In this case, the other validators would vote against approving the block and the block would be retried with a new validator. There is also the potential for the stake of the bad actor validator to be penalized, referred to as 'slashing', such that the network would seize the tokens of a bad actor. As a result of validators generally being paid proportionally to their stake, owners of tokens are able to stake their tokens on behalf of a validator for which the validator pays a yield.

Monetary Policy

It is often inappropriate to think of cryptocurrencies as currencies but in this specific case it is a useful reference point. While most people today interested in forecasting cryptocurrency prices care only about speculation and largely rely on technical trading, the fair value of a token is best thought about in terms of the classical monetary equation of exchange[3].

The typical framework is the following:

1.) A blockchain is created on top of which there are - applications. The compute power needed by the applications are supplied by miners or validators.

2.) In order for a user to use the applications on top of the block chain, the owner of the application demands a fee for the service and the miner or validator demands a fee for supplying computing power.

3.) In the case that useful applications exist on the blockchain, users purchase tokens in order to utilize the applications.

4.) The application owners, miners and validators receive tokens for designing and running the network and participate in a game theory optimization to maximize the value of the tokens they sell back to users.

Sophisticated participants in blockchain ecosystems today by analyzing existing features of a blockchain and future applications are able to plug in reasonable estimates into adapted equation-of-exchange frameworks in order to estimate a *'fair value'* for tokens and make long term investment decisions on a view as to how ecosystems will develop.

Today prices for most tokens are very far from their fair value – most tokens are orders of magnitude too expensive, many of which have a fair value of approximately zero, but some sophisticated venture investors argue that there are a handful of tokens orders of magnitude too cheap on their valuations.

That said, it is worth stating that there is nothing in the methodology above that states that more popular tokens will have high prices in the future or even that as tokens get more popular that their prices should increase. For example, blockchains ecosystems have interest rates and inflation rates, often that change in different regimes. These nuances that may seem small can have strong effects on the long-term fair value of tokens to the point that the effect of debasement of the token on the token's price overrides an expected increase in use of the applications on the chain. Further, it does seems likely that the long-term winners are those blockchains in which token prices do not increase exponentially over time as more value flows to the developers of applications which in turn attracts more users. The point in this case is that rigorous analysis is needed to take any directional view on token price: increased users is by no means sufficient.

2 Through 2021 Solana became a favorite of traditional financial professions primarily due to its speed and secondarily due to the practicality of the chain's founder vs. the highly theoretical and philosophical founders and doctrines of Ethereum and Bitcoin. Unfortunately, Solana has not yet become the panacea solution for a fast, reliable blockchain on top of which all Web3 can be built. In practice the consensus mechanism which Solana leans on to achieve high speeds is less stable than that of the current proof of work systems; today this mechanism entails a rotating but known leader to take on the brunt of transactions with a block. During periods of high volumes (>300k transactions per second on the network) the system has become overwhelmed which has led to a following period of slow processing or even a temporary network halt. The fact that the leader is necessarily publicly known can also lead to directed attacks on the leader which can put the speed and normal functioning of the network at risk.

3 An early yet robust discussion of this concept was written by Chris Burniske in his article Cryptoasset Valuations

Decentralization

Having come this far it is potentially worth drilling down on what the decentralized aspect of blockchains entails. For public[4] blockchains, the full[5] blockchain itself (meaning the actual long line of data that makes up the blockchain) is held by every miner and thus distributed. Equally, anyone meeting the hardware hurdle (which for Ethereum is trivial and possible to do using a cheap laptop) is able to participate in mining. The process of mining involves making public the blockchain and as such the decentralization of the blockchain increases with the number of miners. The concept here is that should some miners be taken offline, the incentive for other miners to begin mining will increase. In this way the ledger is in the public domain and outside of the control of any one entity whether that be a government or a platform, like Facebook/Meta or Banks. This allows for users to interact with each other directly at the cost of a gas fee on blockchains supported by miners with the incentive to protect and maintain the chain through proof or work or proof of stake.

Smart Contracts

In practice smart contracts are nothing more than immutable, executable code written on the block chain. This code is public to all and once written, it is unable to be changed or stopped; as a result smart contracts are often referred to as trustless since one need not trust the counterparty to verify the contract. Weather insurance is a classic example of the application of a smart contract. Consider the following: one person is willing to sell to another person a form of weather insurance: *if 5 inches of rain falls in a single day at Houston Airport before the end of the year, then I will pay you 20eth (Ethereum tokens); otherwise you will pay me 1eth.* Because this a trustless system, both parties place their capital in an escrow account managed by the smart contract, and as a result the smart contract holds a total of 21eth. The buyer and the seller must agree upon a neutral data source for the smart contract to check automatically each day to verify[6] the amount of rain that has fallen at Houston Airport. Perhaps the two parties settle on the NOAA database. Once executed at the end of every day the smart contract checks the NOAA database and follows its instructions: if the day's rainfall is greater than 5 inches, it will automatically send the 21eth to the wallet of the buyer; if the date is greater than the end of the year and there remains eth in the escrow account, the 21eth will be sent to the seller. As smart contracts are simply code, best considered subroutines, they are enormously flexible in what they can achieve in a manner that requires no additional outside engagement by third parties to settle.

Layers

So far we have discussed exclusively what are known as Layer 1 coins or tokens which operate at the base layer on their own distinct chains. In practice the vast majority of Web3 applications are better structured on top of an existing blockchain. Instead, via smart contract chains, blockchains like Ethereum are equipped to handle alternative tokens in addition to their basic utility token. By creating new, distinct tokens on top of an existing blockchain, an entirely new ecosystem can be developed with its own monetary policy. This is generally referred to as Layer 2. The earliest Ethereum Layer 2 ecosystems generally were intended to provide an optional work-around for some of Ethereum's less friendly features, mainly the high cost of executing smart contracts.

For example, Polygon, a Layer 2 solution on Ethereum, reduces the decentralization and security of the Ethereum chain but boosts execution speed and lowers execution prices. Today for most blockchains, these Layer 2 solutions are generally considered necessary to tweak the underlying restrictions of the blockchain in order to build useful consumer applications that can be used quickly and at low cost.

NFTs

For better or for worse (almost certainly for worse in fact), the most popularly known class of Layer 2 tokens are not those that support useful ecosystems, but rather NFTs or non-fungible tokens. Examples include JPEGs of so-called *Bored Ape's* that provide exclusive membership in a consortium of other owners of *Bored Ape* JPEG. Here's the cover image of a Bored Ape NFT (accessed via ipfs.io scanner: https://ipfs.io/ipfs/QmYoWP3Mgvw6cXc9owtpimdoBL2UfZjHVNFtLSpfgVZuk8) that was at least at one point owned by Jimmy Fallon:

[4] *While the vast majority of the blockchains that are likely to become the foundation of Web3 are public, there also exist private Blockchains. Though rarely discussed in the West, the past few years have seen a revolution in private blockchains in China. Because private blockchains do not need to deal with the decentralization problems intrinsic to public blockchains, private blockchains are today much more powerful and applicable than their public peers. As such, government agencies in China have begun adopting blockchain solutions; for example, China's Internet Court which primarily settles ecommerce small-claims disputes uses smart contract settlements. Additional reading on the use of blockchains in the Chinese judicial system here.*

[5] *Full is a meaningful word when it comes to the type of blockchain node. At any point in time a blockchain exists in a certain state. As transactions are added to the blockchain, the state of the blockchain changes. This does not mean that the blockchain is not immutable: the state of the blockchain includes all transactions meaning that any previous state of the blockchain can be calculated given the current state of the blockchain. This compressed version of the blockchain is called a full node. An extended form of the blockchain which consists of snapshots of every state of the blockchain is called an archival node. In practice most nodes are full nodes as these are about 10x smaller than archival nodes. Today the full node of the Ethereum chain is about 700GB while the archival node is about 7TB.*

[6] *The agreed upon neutral data source is generally referred to as an Oracle. In current thought difficult to hack or influence and publicly government databases are generally considered the best oracles though as the demand for Oracles increases, existing knowledgebases like Wolfram Alpha are increasingly palatable, and decentralized custom Oracles solutions like Chainlink are built.*

While an outsider may not understand how anyone could spend hundreds of thousands of dollars on ownership of a graphic that can easily and legally be shared, truthfully these NFTs are best thought of as incontrovertible membership tickets to an exclusive club. While we have copied the image here, only Jimmy Fallon (or the current owner) has the verifiable NFT itself. As to whether its worth it to be in that club, well that is for the market to decide. It appears that many of the high prices we see today are not a result of any fundamental value of ownership but rather a result of buyers hoping to sell their NFT to someone else at a higher price later. Resembling a pyramid scheme, it's doubtful that many of these markets will end well.

That said, NFTs limit the number of tokens available in their layer and could have useful variants down the road. Like all Layer 2 solutions, NFTs are created by means of smart contracts; The majority of NFTs today are created on top of Ethereum which makes them interoperable with Ethereum wallets. This has created demand for NFTs created on top of Ethereum despite NFTs on blockchains like Solana being orders of magnitude cheaper to create[7].

It's often discussed that NFT data is not stored on-chain but rather hosted by a third party platform. Diving into the implication here will help elucidate what NFTs are in the abstract and what more useful variants there might be in the future. When creating an NFT, the contents of the smart contract used in the creation of the NFT is stored permanently on chain. Typically embedded in the smart contract is what amounts to an encoded hyperlink that points to a file hosted externally. For today's archetypical JPEG oriented NFT[8], that metadata will generally consist of attributes like *name* and *description* that would be useful to a wallet displaying an image. That file will also hold a hyperlink that points to a separate image file hosted usually at the same third party hosting the metadata.

Today NFTs have relatively limited use cases but the number is expanding as creators explore what NFTs can achieve. For one, NFT data need not be an image. In a metaverse context an NFT may be soundtrack or animation for an avatar but are likely to become more banal in the more common use cases. For example one could imagine a college issuing LinkedIn badges to graduates proving in an immediately verifiable and trustworthy manner that a person actually graduated with a specific degree from the named university. This would thus enable colleges to provide something of significant value to their own graduates while also cutting down on resume fraud. In many of these data-heavy cases NFTs are likely to be priced very cheaply, on the order of cents, and useful to the user through their portability. Most likely this class of NFT is unlikely to be traded but rather purchased and held indefinitely as would be usual for a typical physical consumer good.

Potentially more powerful in the near term are data-lite NFTs that are used as exchangeable, lasting social tickets or receipts. Consider two areas of relatively low hanging fruit: influencer ticketing and rewards programs. In the case of influencer ticketing, a musician might issue tickets in the form of NFTs which can be verified via smartphone at the venue. This would mean tickets are transferable and thus able to be resold but in order to reduce the incentive for scalping the musician might build in an additional, escalating transaction fee (maybe paid to a charity or to the musician themselves or even to the holders of tickets never resold) whenever a ticket is resold. In this way we are achieving the Web3 promise of *read-write-own*. Following the performance, the musician might send those holding tickets an additional image-based NFT to commemorate the night.

7 To some extent this might be part of the point – nontrivial cost of creating NFTs on the Ethereum chain itself produces a element of artificial scarcity. Potentially an underappreciated risk to today's NFT pricing regime would be Ethereum's long awaited upgrade from proof-of-work to proof-of-stake. This upgrade should lower gas prices by an order of magnitude which would in turn make the creation of NFTs more accessible and more practical in larger scale, which may in turn result in a general devaluing.

8 Though separate from this discussion of Web3, conversations around the relation of NFTs to art are generally unnecessarily inflammatory. Some of the few moderately insightful can be found in the art criticism publication Caesura: CAESURA ROUNDTABLE: THE NFT and WHY THERE IS NO GOOD NFT ART (YET?)

On the next tour through the same city the musician might offer a discounted sale of tickets to those still holding never resold[9] tickets from the first show. In practice the public nature and non-fungibility of NFTs can be leveraged as community building tools.

The case of rewards programs is potentially more banal but easier to map to monetary incentives. Consider that a group of independent coffee shops in a city coordinate to create a shared rewards program that will incentivize customers to visit the group of shops. Instead of building out a shared network on the cloud, the consortium decides a public ledger will be easier to operate through and thus they launch a very simple blockchain for which the basis token is distributed on the purchase of a coffee and can be utilized to pay for coffee, not unlike the Starbucks star system. On top of this system potentially some coffee shops decide to issue NFTs for the purchase of special drinks. Further NFTs themselves can be programed to issue their own tokens[10] at predetermined frequencies for predetermined periods – potentially in this case the coffee shops might produce a seasonal NFT which produces tokens exchangeable for seasonal drinks and offer this seasonal NFT at a discount.

Concluding Thoughts

There are many in the Web3 ecosystem naively speculating, often out of greed, in the hopes of achieving great wealth by selling to some greater fool at a higher price. Some have been or will be incredibly successful though the story will likely end badly for many.

There is a steep learning curve in building the new generation of the web and as a result so far most applications developed to date have a 'Hello World' quality – seemingly simple and somewhat silly announcements of what's possible if not actually useful. And many of these 'Hello World' applications seem to be exchanges and marketplaces for tokens and NFTs. While it takes a non-zero amount of good faith to look beyond a landscape littered with limited use applications to examine the types of non-trivial use cases possible once developers get their feet under them, it's worth watching the space for emerging practical applications and business models. We are also actively looking for opportunities, generally only available in private markets, to invest behind companies capable of providing tools to the next generation of application developers –picks and shovels to the current goldrush. Some big publicly traded players are also likely to benefit from the development of Web3, though their market caps currently are so huge that at this stage this only presents a modest tailwind to company earnings.

As to allocating money to cryptocurrencies themselves, we continue to view this as highly speculative at this stage. Could certain crypto tokens go up a lot in value from here? Absolutely. But many that have value today will likely see their value fall, possibly even to zero. For those who enjoy speculation or who think they are good at it, Crypto provides an exciting opportunity. We, however, do not speculate in markets on behalf of our clients. We invest with long-term, universal and fundamental principles at the foundation of what we do; we are trusted by our clients to place their money into financial markets in a manner that will enable them to achieve their long-term financial objectives. In this context, while we're happy to discuss how to manage and contain speculative risk, we won't be allocating client portfolios to specific cryptocurrencies in the near future.

Some financial advisors appear to be jumping on the crypto bandwagon. They argue that cryptocurrencies offer protection against inflation and monetary debasement. But as we anticipated, and has become self-evident recently, cryptocurrency prices aren't a hedge to inflation or a store of wealth. They largely march to their own beat and to the extent they are correlated to other financial assets, it is to other highly speculative securities like unprofitable growth tech stocks. After all it tends to be the same people, often on leverage, who trade both the most speculative stocks and Crypto. Thus, there is significant risk that a sell off in one creates a selloff in the other. If anything, this dynamic makes Crypto negatively correlated to inflation and a dangerous place to store wealth. For example, as fear of a Russian invasion of Ukraine has increased, we've seen highly correlated sell off in both equities and cryptocurrencies. Further as inflation has risen and central banks have started to make noise about tightening monetary policy, crypto prices have fallen as have growth tech valuations and other highly speculative investments because real interest rates have started to rise. While we don't know for sure given the tremendous uncertainty described above, our guess would be that if inflation stays high and real interest rates continue to rise, cryptocurrency prices will continue their downward trajectory. Speculative assets always struggle in the context of rising real rates. That said, Web3 has a variety of potentially exciting implications as we've described above and we'll continue to look for attractive investment opportunities as this new generation of web technology develops.

[9] *The never-resold idea is an emerging concept in NFT's. Read more about this concept here*

[10] *This is a feature of NFTs only recently being explored but has the potential to produce interesting solutions and dynamics.*

Important Disclosures

THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY AND SHOULD NOT BE RELIED UPON AS INVESTMENT ADVICE. *This document has been prepared by GenTrust and is not intended to be (and may not be relied on in any manner as) legal, tax, investment, accounting or other advice or as an offer to sell or a solicitation of an offer to buy any securities of any investment product or any investment advisory service. The information contained in this document is superseded by, and is qualified in its entirety by, such offering materials. This document may contain proprietary, trade-secret, confidential and commercially sensitive information. U.S. federal securities laws prohibit you and your organization from trading in any public security or making investment decisions about any public security on the basis of information included in these materials.*

THIS DOCUMENT IS NOT A RECOMMENDATION FOR ANY SECURITY OR INVESTMENT. *References to any portfolio investment are intended to illustrate the application of GenTrust's investment process only and should not be used as the basis for making any decision about purchasing, holding or selling any securities. Nothing herein should be interpreted or used in any manner as investment advice. The information provided about these portfolio investments is intended to be illustrative and it is not intended to be used as an indication of the current or future performance of GenTrust's portfolio investments.*

PAST PERFORMANCE IS NOT INDICATIVE OF FUTURE RESULTS OR A GUARANTEE OF FUTURE RETURNS*. The performance of any portfolio investments discussed in this document is not necessarily indicative of future performance, and you should not assume that investments in the future will be profitable or will equal the performance of past portfolio investments. Investors should consider the content of this document in conjunction with investment fund quarterly reports, financial statements and other disclosures regarding the valuations and performance of the specific investments discussed herein.*

DO NOT RELY ON ANY OPINIONS, PREDICTIONS, PROJECTIONS OR FORWARD-LOOKING STATEMENTS CONTAINED HEREIN. *Certain information contained in this document constitutes "forward-looking statements" that are inherently unreliable and actual events or results may differ materially from those reflected or contemplated herein. GenTrust does not make any assurance as to the accuracy of those predictions or forward-looking statements. GenTrust expressly disclaims any obligation or undertaking to update or revise any such forward-looking statements. The views and opinions expressed herein are those of GenTrust as of the date hereof and are subject to change based on prevailing market and economic conditions and will not be updated or supplemented.*

EXTERNAL SOURCES. *Certain information contained herein has been obtained from third-party sources. Although GenTrust believes the information from such sources to be reliable, GenTrust makes no representation as to its accuracy or completeness. Logos are protected trademarks of their respective owners and GenTrust disclaims any association with them and any rights associated with such trademarks.*

THIS DOCUMENT IS NOT INTENDED FOR GENERAL DISTRIBUTION AND IT MAY NOT BE COPIED, QUOTED OR REFERENCED WITHOUT GENTRUST'S PRIOR WRITTEN CONSENT.