Perspective from **Franklin Templeton Industry Advisory Services**

Understanding Web3—a primer on the emerging digital asset ecosystem

June 2023

The purpose of this primer

The technology underlying Web3 and emerging digital assets enables new ways of transacting and brings with it new models of participation and innovation. Understanding how these models and capabilities differ from traditional commercial and financial practices requires familiarity with some new concepts and terminology.

This primer will provide an overview of digital assets, and related terms and technology. Its aim is to equip the reader with the foundational understanding necessary to appreciate the potential impact on the future of the financial industry, but also on economies and society more widely. This document does not pre-suppose any technical knowledge but rather is aimed at individuals who are curious and looking to understand more.

Table of Contents

There are also additional publications that may prove useful once the foundational concepts are clear. These include all articles on technology and disruption at the Franklin Templeton Institute: Disruptive Technology web page. Specifically,

- Technology-driven megatrends part I: The evolution of commercial technologies and impact on business delivery
- Technology-driven megatrends part II: 5 tech-driven megatrends transforming society.

Introduction

Web3 and the emerging digital asset ecosystem represent a departure from traditional commercial and financial practices. Understanding the basics of the new domain may require some level-setting for those less familiar with this space.

At its core, Web3 and the emerging digital asset ecosystem look to replace intermediaries and empower users directly. This marks an extension of trends begun back with the launch of the internet. Web1 laid the rails of the information superhighway, providing users direct access to websites offering previously unimagined amounts of data, access to knowledge, and connectivity. Web2 shifted the customer experience of the internet, combining new mobile technologies with information networks to allow the upload of user-generated content and leveraging the power of big data and nascent AI technologies to personalize and tailor the delivery of content via specialized apps.

Web3 looks to change the participation model, rewarding those that contribute time, resources and effort to drive internet activities and eliminating the frictions, costs and controls that intermediaries may layer into transactions. To accomplish this aim, the emerging Web3 digital asset economy has set up a new way of doing business. Those that have developed the protocols and apps that are defining the space use a variety of tokens to orchestrate activity and then record the resulting transactions on a new type of ledger that distributes information simultaneously across a whole network of participants.

It is initially useful to think of the ecosystem having four fundamental elements: blockchains, tokens, smart contracts and wallets.

Foundational building blocks of Web3

Blockchains

Blockchain is the underlying technology of the Web3 ecosystem. Traditionally ownership of an asset is recorded centrally in a private ledger. Changes in ownership are reflected by updating the ledger entry. Typically, only the central authority managing a ledger has visibility across the entire set of entries. An individual's visibility is restricted to their individual accounts and transactions. Think about your current bank. The bank has a ledger showing all the checking and savings accounts of its entire customer base. The bank sees the entire set of accounts and all the transactions that occur. You only see your own accounts. Another bank—even one where you may have an account—cannot see any of the other bank's accounts or transactions.

Blockchain ledgers operate differently. A blockchain is a digital record or ledger of transactions, duplicated and distributed across an entire network of computer systems. Blockchains represent complete records of all transactions ever performed within a system. The entire progression of transactions, stretching back to the very first (genesis) trade, is maintained.

Every node in the blockchain network has a real-time, updating copy of this ledger. Every node sees new transactions coming through and can view the entire history of transactions. Because of this broad transmission, a blockchain is also sometimes described as a "distributed ledger technology" or DLT.

Using the bank analogy, it would be as if all the banks had one ledger that showed the whole universe of checking and savings accounts, and every bank could see real-time movements of money into and out of these accounts as well as the whole history of transactions that occurred in these accounts.

How do blockchains work?

Blockchain ledgers are comprised of "blocks" of transactions that are "chained together" to create an unbroken record of the activities that have occurred. Unverified transactions are queued up to be verified. Verification consists of checking to be sure that the buyer has sufficient currency to pay for the transaction and that the seller is properly set up to receive the transaction. Each time a transaction is verified, it is added to a block.

Each block holds a pre-specified amount of data. A block can be filled with many small transactions (that take up little bits of data storage) or with just a few large transactions (that take up a lot of data storage). Think about when you try and send a file via email—some files are big and require a lot of bandwidth to transmit, and others are small and can be sent easily. When enough verified transactions are put into a block and the data limit is reached, the verifier notifies other nodes in the network that a block is ready to be added to the chain.

Because the ledger is distributed and immutable (once a block is added to the chain, it is there forever), nodes in the network must have confidence that the block and its transactions are accurate before it can be added. To obtain such confidence, a "consensus" must be reached across the nodes in the network that the block is good to go. There are different types of consensus mechanisms utilized to reach such consensus.

It is the collective work of validator nodes that results in an update to the transaction record, rather than a single central institution approving the transaction and updating the ledger. There is no notion of or requirement for licensing because every transaction is transparent and effectively checked by the other nodes in the system before it is written into the ledger.

Consensus mechanisms

There are two primary consensus mechanisms currently used by blockchains in the Web3 ecosystem—proof-of-work (PoW) and proof-of-stake (PoS).

In PoW blockchains, such as Bitcoin—the largest and original blockchain—validators, or "miners," race to solve an increasingly complex cryptographic puzzle. The winner of this race gets to add the block to the chain and earn the block "reward" for having done so. The reward is paid in the native currency of the blockchain. The network automatically mints new currency to pay the miners. This is how the money supply increases in a proof-of-work blockchain.

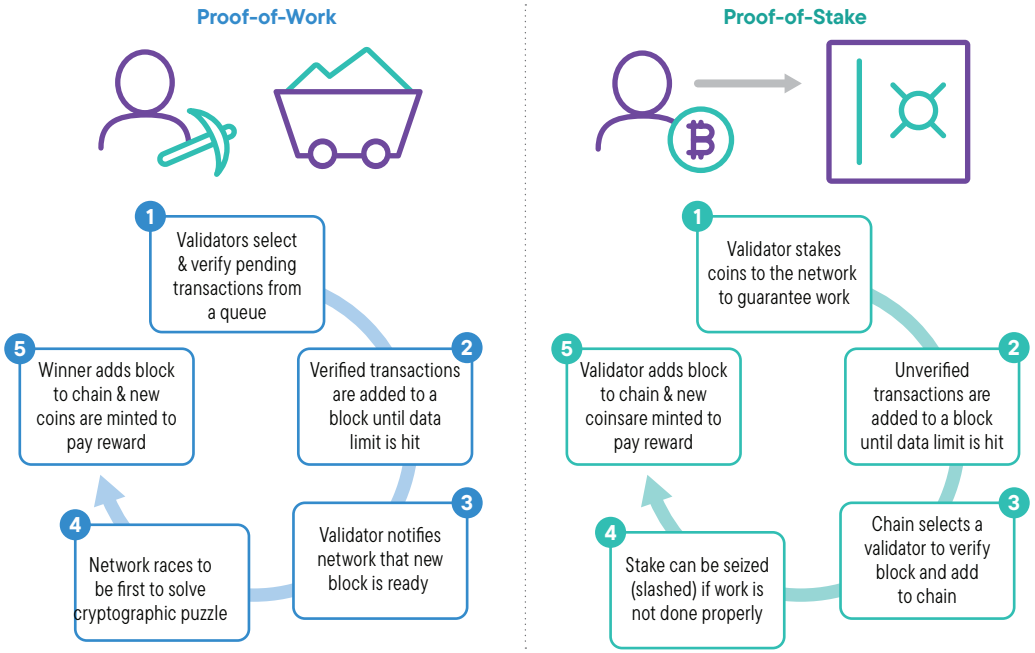
When a blockchain is launched, the reward tends to be high in order to attract validators. As activity on the blockchain increases, the size of the reward decreases because blocks are being added and rewards are being paid out more frequently. This happens at predictable intervals when the size of the blockchain reaches certain thresholds. For Bitcoin, this reduction in the reward size is called a "halving" because the size of the reward gets cut in half each time.

The complexity of the cryptographic puzzle also increases in line with the blockchain's transaction activity. In the beginning, it is easy to solve the puzzle required to add a block to the chain in order to encourage new validators to join the network. Over time, there is growing competition to verify a block, so the puzzle becomes harder, and more processing power is required to win the race.

More processing power means that more energy is required to run the calculations. This has led to concerns about the ESG impact of PoW blockchains, especially Bitcoin. Other blockchains have thus developed a different consensus mechanism—PoS. Overall, seven of the ten biggest blockchains use PoS. The second largest blockchain, Ethereum, switched from PoW to PoS in September 2022.

Proof-of-work is contrasted with proof-of-stake in Exhibit 1.

Exhibit 1: Overview of Top Consensus Mechanisms Used to Verify Blockchain Transactions



Source: Franklin Templeton Industry Advisory Services. For illustrative purposes only.

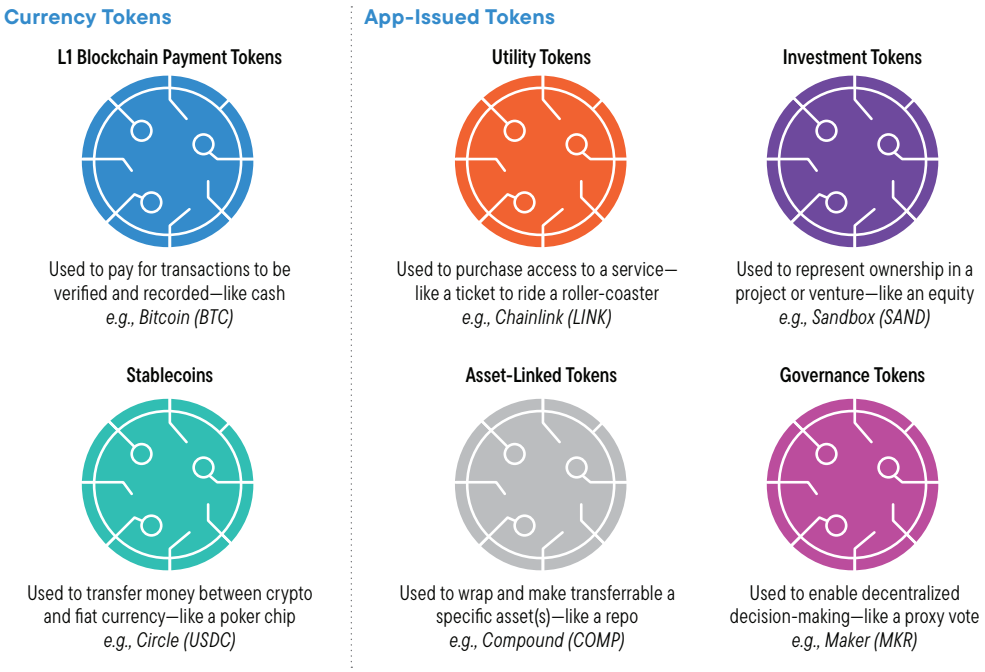
PoS networks do not rely on solving a cryptographic puzzle or on competition between nodes to validate blocks. Instead, they require validators to commit their own capital (put up a stake) and risk losing portions of their deposit if they allow an inaccurate block to be created. The stake is locked up by the blockchain for the entire period that the node wishes to be included in the verification process. This lockup is analogous to funds being segregated in an escrow account. The fact that the validator risks being penalized and losing a portion or all their capital (known as "slashing") if they fail to perform their work accurately is seen as sufficient incentive to trust their work when they add a block to the chain.

The larger the stake, i.e., the more capital put at risk, the higher the probability of that validator being selected by the protocol to verify a new block of transactions and earn a reward for doing so successfully. In this way, those with most to lose are most involved in the operation of the system and validators become increasingly invested in the integrity and continued operation of the system.

Tokens–what are they and what are the different types of tokens?

Tokens play a critical role in the Web3 digital asset ecosystem. They are used for many different purposes. Tokens are used to facilitate payments, initiate services, bestow ownership, authorize voting, convey rights and transfer assets. Specialized tokens are used for each of these functions. Broadly, these specialized tokens can be broken down into two categories: currency tokens and app-issued tokens as shown in Exhibit 2.

Exhibit 2: Overview of Web3 Digital Asset Token Types



Source: Franklin Templeton Industry Advisory Services. For illustrative purposes only.

Currency tokens—cryptocurrencies, stablecoins & CBDCs

A cryptocurrency or payment token is used for payments in the Web3 digital asset economy, just as government issued fiat currencies such as the US dollar, euro or Japanese yen are used for payments in today's economy. Just like each nation in the world today may choose to issue its own government-backed currency, each blockchain can also issue its own cryptocurrency in the form of a token. The term cryptocurrency is used because these monies are cryptographically protected so that each token can be identified and tracked to prevent unauthorized movements. These currency tokens fulfil three main use cases.

- Cryptocurrency tokens are minted by the blockchain and paid as a reward to network participants that verify transactions within the ecosystem;
- Participants that transact within the ecosystem must pay in the ecosystem's native cryptocurrency token to have their transaction recorded;
- Cryptocurrency tokens can also be used as an asset that can be staked, loaned, borrowed, or posted as collateral in certain types of financing apps.

The biggest and best-known cryptocurrency token is bitcoin (BTC)—the native currency of the Bitcoin blockchain ecosystem. As of May 9, 2023, bitcoin has a market cap of $536 billion and a 24-hour trading volume of $15 billion.[1] Over 15,000 businesses around the world accept Bitcoin as payment, and there are more than 36,000 bitcoin ATMs in the United States.[2]

Ether (ETH), the native token of the Ethereum blockchain ecosystem, is the other leading cryptocurrency token. The market cap of Ether on May 9, 2023, was $222 billion with a 24-hour trading volume of $7 billion.[3] Other leading blockchain ecosystems with their own cryptocurrencies include Cardano (ADA), Solana (SOL), Polkadot (DOT), Polygon (MATIC) and Avalanche (AVAX).

None of these cryptocurrency tokens can be directly exchanged for US dollars or other government issued fiat currencies. To facilitate movement of funds between the traditional and the crypto economies, a new financial instrument has been developed—stablecoins.

Stablecoins are a type of token that has its value pegged to another currency, commodity or financial instrument. An investor holding bitcoin, ether or another cryptocurrency can exchange that cryptocurrency token for a stablecoin. The most widely used stablecoins are Tether (USDT) and USD Coin (USDC). These tokens seek to tie their value to the US dollar. One USDT or one USDC should equal one US dollar. The collateral pools associated with these stablecoins are primarily comprised of government issued fiat currencies or fiat currency denominated securities. The collateral pool is managed by an investment team or by sub-advisors that the stablecoin provider selects. There are also stablecoins such as DAI from the MakerDAO protocol that also pegs its value to the US dollar, but their collateral pool can include cryptocurrencies or crypto tokens and is algorithmically managed.

Stablecoin owners have several options on how to utilize their tokens. They can simply hold them and maintain their balance in that stablecoin to reduce their exposure to any underlying cryptocurrency or token. They can exchange the stablecoin for another cryptocurrency or token or they can redeem their stablecoin. Upon redemption, the stablecoin is "burned" or destroyed and the underlying collateral value (one US dollar per stablecoin in the examples above) is extracted from the collateral pool and deposited into the holder's account.

Stablecoins whose collateral pool is comprised solely of fiat currency or fiat currency denominated securities would thus be able to have those assets returned to the client—thus providing an off-ramp for assets from the crypto ecosystem back into the traditional economy.

At present, there is no regulation requiring stablecoin holders to guarantee that the requisite amount of collateral is held to ensure that the peg remains stable. Nor is there any requirement for stablecoin providers to offer transparency into their stablecoin holdings for investors to evaluate the collateral pool. Moreover, today's stablecoin providers are not prohibited from investing in higher risk assets to improve the return on their collateral pool, and there is no requirement for them to share any yields they earn from the collateral pool with the stablecoin owners. Indeed, most stablecoin providers keep those excess returns for their own benefit. Each of these considerations add risk to the use of stablecoins and may soon be addressed by regulators based on draft legislation and ongoing discussions.

Central bank digital currencies (CBDCs) are another type of currency token that would represent fiat currencies rather than cryptocurrencies. These offerings are under development or investigation by major central banks around the world. As digital versions of a sovereign country's fiat currency, CBDCs would represent a claim on the issuing nation's central bank and, ultimately, on the issuing government itself. Depending on their implementation, CBDCs may also offer opportunities for payments and for moving money between the digital and fiat worlds. While CBDCs have been issued by a handful of small countries they have not yet been issued by the main global economies.

Decentralized app-issued tokens

While currency tokens are used for payments, developers who build applications (apps) on a blockchain (decentralized apps) also have the option of creating their own token to fulfill other purposes. There are four main types of tokens that are issued by decentralized apps: utility tokens, investment tokens, governance tokens and asset-linked tokens.

- *Utility tokens* are used to gain access to and enable consumption of a protocol's services or to bestow certain privileges. Utility tokens are akin to buying a ticket to gain entry to or access a fairground ride. For example, a user can buy a LINK token to access the Chainlink app which provides market, weather, and sports data and has enabled transactions valued at $6.9 trillion.[4] Alternatively, utility tokens can be purchased to access special benefits such as fee discounts. In this way they are like transferrable loyalty points.
- *Investment tokens* represent ownership in a project or venture and can be thought of as the equivalent of shares of equity. For example, those wishing to own land in the Sandbox Metaverse receive SAND tokens that represent the value of their digital parcel. Oftentimes, projects that are just starting up will issue investment tokens to raise capital for their venture and provide a set of these tokens to the early participants and funding partners. The hope with investment tokens is that the value of that token will increase over time, offering owners a profit potential.
- *Governance tokens* are distinct from ownership tokens. Governance tokens permit the holder to vote on issues pertaining to the app's underlying protocol (open access code base), its business practices, and its strategic direction. Because apps in the crypto domain are decentralized and typically run by a foundation, there is not a centralized management team to make these types of decisions. Instead, the community of governance token holders are often invested with the authority to make decisions on behalf of the app. For example, owners of the MAKER token are permitted to vote on issues pertaining to the MakerDAO protocol that issues and manages the DAI stablecoin. Proposals put forward to the MAKER community might include topics such as accepting a new type of asset for the collateral pool, adjusting the rules of the algorithm that manages the stablecoin, or hiring a new head of marketing. Each time a proposal is put forward, the holders of the governance token are asked to vote, and if a 51% majority of those who vote approve, the proposal is passed.
- *Asset-linked tokens* can be issued directly by a decentralized app or they can be minted by asset owners via a decentralized app. These tokens transfer ownership of an underlying asset and include an embedded contract that describes the ownership terms and the utilization rights that will be provided to the token holder. There are a wide variety of asset-linked tokens in the crypto domain. Decentralized exchanges and financial apps mint asset-linked tokens and issue these tokens to specific contributors to acknowledge the collateral they have given to their protocol and list the fees or rewards they are entitled to receive. These tokens are like a repurchase agreement (repo) contract. Other platforms allow creators to issue their own asset-linked tokens that provide ownership and utilization rights for a specific digital asset such as digital content or art. Owners of physical assets can also create non-fungible tokens (NFTs) to cover a variety of offerings from collectible trading cards to exclusive fashion items to property.

In addition to their designated use, each of these token types—utility, investment, governance, and asset-linked—can also be loaned, borrowed, and posted as collateral within the crypto ecosystem. This expands the utility of the tokens, giving them dual purpose as both a transactional vehicle and a financial instrument.

Moreover, app-issued tokens are programmable using the third key building block of the crypto ecosystem—smart contracts.

Smart contracts

Because tokens are essentially software, they are "programmable." The code can specify their terms, describe how and when those terms might change, and designate the rights that owning the token might convey. This programmability can also extend to describing actions to be initiated when a specific set of conditions are met—essentially an "if-then" scenario. For example, a token could be programmed to provide the holder 1% of the income generated by an artist's royalty pool and additional instructions could be coded to pay out those monies each time a new royalty check is cut.

These instructions are laid out in a new offering called a "smart contract." Smart contracts are self-executing contracts in the form of code that is housed on a blockchain. Just as a transaction is recorded on the blockchain, the terms of the transaction are also recorded on the blockchain. A "virtual machine" (basically an in-blockchain computer) monitors the terms of the smart contract, and when specific inputs are received, the smart contract sends its commands to the computer to be enacted. This happens automatically without manual intervention.

Many different types of triggers can be programmed to initiate the self-executing activities of a smart contract. An employee of a decentralized app may have their payroll administered via a smart contract that distributes their paycheck on the 1st and 15th of each month; a lending pool may set up smart contracts to pay the providers of liquidity their proportionate share of interest each time an interest payment is collected from those who borrow coins; the owner of a skin for a particular avatar in a gaming app can set up a smart contract that allows them to loan that skin to another player and receive payments until the end of the loan term. The trigger data may come from transactional activities recorded on the blockchain or from a specialized protocol called an oracle, which collects and sends data to smart contracts from the external world.

The ability to program conditionality into a smart contract and wait for the right trigger enables programmers to deliver a huge potential array of "if-then" scenarios. As such, smart contract algorithms can be used to automate many commercial interactions and service provisions. Smart contracts can eliminate the need for intermediaries, greatly reducing costs, resources and the time required to process a transaction or enforce an agreement.

Smart contracts direct the provision of payments and other benefits not to individuals or institutions, but to digital wallets—the fourth and final foundational building block of the crypto ecosystem.

Digital cryptocurrency wallets

Token owners must have a digital cryptocurrency wallet to participate in a blockchain ecosystem. This wallet is essentially a piece of software that provides an interface between the owner and the blockchain.

This digital cryptocurrency wallet is very different from a traditional checking, savings, or investment account. It is also very different from off-chain digital wallets such as an Apple or Google wallet that contains a masked version of a user's credit card.

Digital cryptocurrency wallets are simply addresses on the internet where assets can be stored. There is no identifying information on these wallets other than a long string of letters and numbers. The wallet itself contains a digital key that is required to unlock and access the holdings in the user's wallet, and such keys are only shared when a user authorizes a transaction. An apt analogy is to think of a user's assets as being in a safe deposit box in a bank vault. The box is identified only by its number, and the user is the only one with the key to open or close their box.

As such, the custody and security of digital assets means protecting the digital keys that unlock the wallet to enable a ledger to deposit and/or "move" an asset. For now, many novices engaged in the crypto ecosystem delegate custody and rely on centralized exchanges to hold their crypto tokens on their behalf—a practice that is not allowed in regulated security markets because of concentration risks and the potential for misappropriation of customer assets. More experienced participants typically opt for self-custody. Indeed, a saying in the crypto space cautions, "Not your key, not your crypto." Institutional grade infrastructure is being rapidly built out for digital keys, however, to provide appropriate levels of security, confidence, and safe-keeping. As these offerings emerge, there may be a shift away from the self-custody model.

Digital cryptocurrency wallets can have two states. They are said to be "hot" when they are connected to the internet, and access to the keys is protected by the wallet software. By contrast, cold storage refers to *physically* protecting the keys, e.g., in a physical vault, like gold. Typically this is done via a storage device that can be plugged into the internet, like a USB stick. Hot storage has the advantage of convenience and speed of access, but that comes at the cost of lower security, so hot wallets tend to contain minimal transactional balances. Cold key storage tends to be used for those assets/balances that owners do not need to immediately access.

While the personal information associated with a digital asset wallet is anonymous and only a user's IP address is displayed, the activities that take place in an individual's wallet are fully transparent. Each movement of an asset out of one wallet and into another is recorded on the blockchain as a transaction and is thus distributed and viewable by every node on that network. For this reason, the crypto ecosystem is said to be "pseudo-anonymous" rather than fully anonymous.

Understanding the Web3 digital asset ecosystem

Before we explain the Web3 digital asset ecosystem in more detail, it is worth pausing to put it into perspective. On May 9, 2023, its market cap was $1.1 trillion, with a daily trading volume of $33.5 billion.[5] As of May 15, there was $47 billion locked in smart contracts[6] and roughly the same all-time trading volume across the top 5 NFT marketplaces.[7]

Significantly, even at the height of the "Crypto Winter" when cryptocurrency prices were languishing, and in the wake of the FTX blow-up and recent bank runs, the underlying crypto ecosystem continues to exhibit a high degree of resilience and to sustain high levels of developer interest, a harbinger of future innovation. For example, in 2022, when the value of many tokens fell by 70% or more, monthly active developer count grew 5% reaching a new all-time high.[8] It is also not just about developers flocking in and jumping on the bandwagon of the latest thing: Ethereum retains 30% of all full-time developers who joined after 2017.[9]

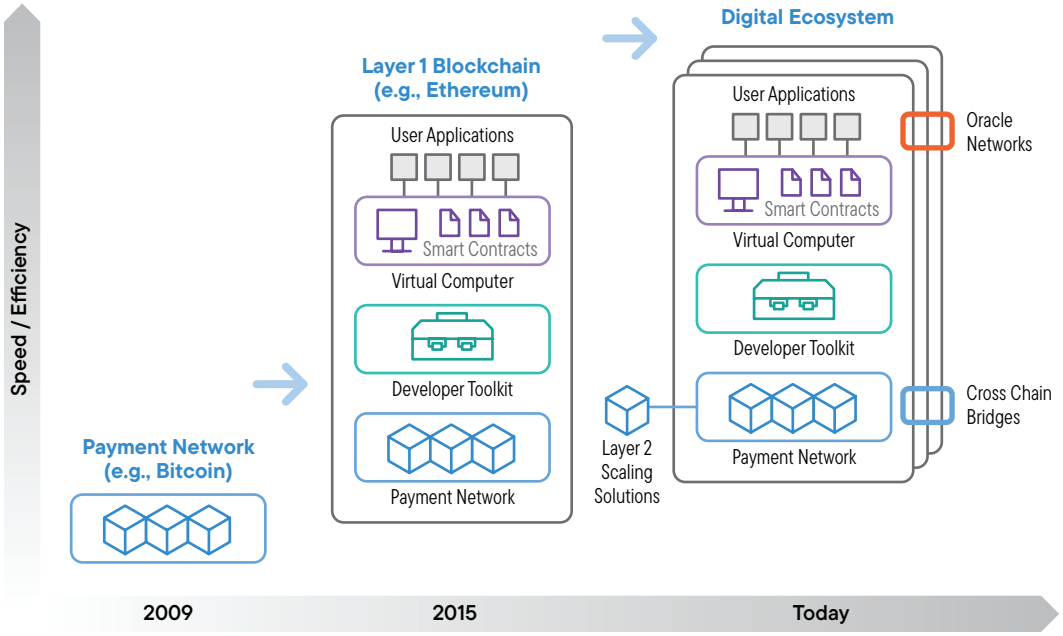
Ecosystem evolution

Today's Web3 digital asset ecosystem can trace its roots to the Cypherpunk movement that began in the 1980s. This movement brought together a community of computer scientists and academics that felt alarm at the loss of privacy they saw occurring as a result of computers and emerging network technologies. They envisioned a world where individuals could transact with privacy, keep their personal information confidential—from both governments and corporations–and eliminate the ability of intermediaries to act as gatekeepers.

Several innovations were created by those associated with the Cypherpunk movement to help achieve those aims in the period leading up to 2009. These advancements and more background on the movement are detailed in our Megatrends Part I white paper, The evolution of commercial technologies and impact on business delivery. Such innovations set the stage for the emergence of Bitcoin in 2009.

The launch of the Bitcoin network and the bitcoin payment coin was the seminal event that laid the foundation for today's crypto economy. As illustrated in Exhibit 3, however, it was only the first such innovation. The speed of change in the ecosystem has been rapid, and today's landscape looks quite different. Understanding the evolution of crypto offerings is critical to appreciating the economic potential of the new offerings and separating out the volatility of individual coins and tokens from the vitality of the growing ecosystem.

Exhibit 3: Evolution of the Web3 Digital Asset Space



Source: Franklin Templeton Industry Advisory Services. For illustrative purposes only.

Bitcoin and payment networks

In the white paper that introduced Bitcoin, published in October 2008 by Satoshi Nakamoto, the anonymous creator(s?) of Bitcoin, the author described their vision as a peer-to-peer electronic cash system. Nakamoto wrote, "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."[10]

"Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments,"[11] Nakamoto noted. He then posited that "while the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads,"[12] he concludes.

Nakamoto then lays out his mission statement: "These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party. What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[13]

Many of the elements to enable this vision had already been pioneered by Cypherpunks as noted in our earlier white paper. These included programmable electronic money, the proof-of-work approach to verifying transactions, and the idea of a shared ledger. Bitcoin took these innovations a step further, introducing blockchain and the idea of a distributed ledger, and defining the process for moving digital money from one wallet to another wallet to avoid double-spending—thus enabling a new concept called digital scarcity.

Bitcoin was officially launched in early 2009, becoming the first fully developed implementation of a crypto service. It was unclear, however, what the use cases for bitcoin would be as there was no commerce running on any crypto rails.

Layer 1 (L1) blockchains

Just a few years later, in 2014, another visionary, Vitalik Buterin, laid his vision on how to rectify that problem and create a platform to enable the development and deployment of decentralized applications to enable commerce. He wrote that the designer(s?) of Bitcoin "desired to test two parameters—a trustless decentralized database enjoying security enforced by the austere relentlessness of cryptography and a robust transaction system capable of sending value across the world without intermediaries. Yet the past five years have painfully demonstrated a third missing feature: a sufficiently powerful Turing-complete scripting language."[14]

He went on to announce his plans for the Ethereum network. "Ethereum," he explained, "is a modular, stateful, Turing complete contract scripting system married to a blockchain." The goal of the model was "to provide a platform for decentralized applications—an android of the cryptocurrency world, where all efforts can share a common set of APIs, trustless interactions and no compromises."[15]

Put more simply, Ethereum set out to build a new open-source development platform on top of a blockchain payment network where programmers could develop a whole array of applications to operate in a decentralized manner. His model for this vision was the Android platform that was launched in 2007 by the Open Handset Alliance, a group of prominent companies that includes Google, HTC, Motorola, Texas Instruments and others.

Yet, unlike apps created by Android developers that relied on third-party platforms such as Google to host their offerings and fiat currency banking and payment rails to process their transactions, Ethereum would allow apps to be launched directly by developers on the decentralized Ethereum network and transactions to be facilitated by an embedded peer-to-peer cash payment network akin to Bitcoin.

Ethereum added to the innovations first introduced by Bitcoin. The Ethereum platform introduced its own programming language and developed a toolkit for programmers which included templates to create their own programmable tokens and to design their own "if-then" functionality via smart contracts. The platform launched the "Ethereum Virtual Machine" or EVM—a cloud-based processing computer that was designed to monitor the state of transactions by continually assessing "if-then" clauses laid out in the smart contract code and initiating actions when the correct triggers were identified. Finally, Ethereum replicated the peer-to-peer cash payment network first introduced by Bitcoin and introduced their own native cryptocurrency—ether.

By April 2023, Ethereum had over 4,000 decentralized apps running on its platform, with balances worth almost $3.0 billion held in the smart contracts of its top 10 decentralized apps.[16] On May 9, 2023, Ethereum's 24-hour trading volume amounted to more than $6 billion in transactions.[17] Apps on the platform ranged from decentralized cryptocurrency exchanges to marketplaces that allow users to mint their own NFTs and/or swap their own collectibles to decentralized financing apps that facilitate the borrowing and lending of cryptocurrencies to gaming apps, gambling apps, and social media apps.

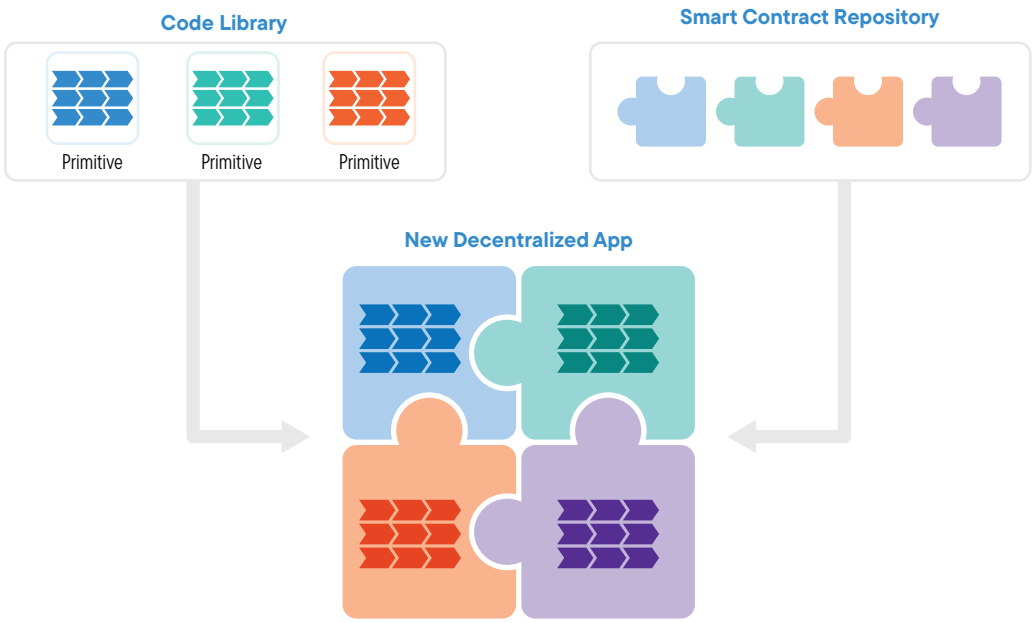
Over time, this collection of capabilities—1) an embedded native peer-to-peer cash payment network, 2) a common developer coding language and toolkit, and 3) a virtual computer able to host decentralized apps and facilitate the automated execution of smart contract clauses—became the blueprint for a self-contained crypto transactional ecosystem. These platforms have subsequently come to be known as a Layer 1 or L1 blockchain.

By April 2023, several L1 blockchains had emerged, each supporting their own economic ecosystem. As of May 9, leaders included Cardano (ADA) with a $13 billion market cap; Solana (SOL) with an $8 billion market cap; Polkadot (DOT) and Tron (TRX) both with a $6 billion market cap; and Avalanche (AVAX) with a $5 billion market cap.[18] In a sense, these L1 blockchains can be thought of as digital nation-states with their own currencies, economies, and payment systems.

Collectively, these L1 blockchains have set a new standard for how app development can occur. This is illustrated in Exhibit 4 on the next page.

Each L1 blockchain offers developers a set of composable open-source building blocks. Commonly used processes such as "make a market between these two assets" or "loan this asset to a specific borrower" become primitives where the entire set of code can be lifted in its entirety from the platform's code library and plugged in to a new app's code base, accelerating the developer's ability to design and launch a new offering. This "Lego-like" ability is possible because all apps on the same platform use the same programming language and the smart contract templates offered on the platform are interoperable. Thus, new apps can adapt existing primitives, interact with existing apps, and enable new functionality more rapidly.

Exhibit 4: Composability and Interoperability in Decentralized App Design



Source: Franklin Templeton Industry Advisory Services. For illustrative purposes only.

The reuse and composability of code primitives accelerate progress by avoiding unnecessary and costly reinvention and create a Darwinian situation where the best code for a particular process will quickly be used by everybody. Indeed, the primitives that are being developed on L1 blockchains have been tested in so many apps that are running 24 hours a day, 7 days a week, 365 days a year that for many, they have moved beyond being seen as software to a whole new category called "trustware."

Unsurprisingly, the ease of coding new apps and the opportunity to keep a larger percentage of the revenues generated by an app by not having to pay a platform hosting fee are drawing significant developer talent to the L1 blockchains. As of January 2023, Electric Capital noted in their annual Developer Report that between 2018 and 2022, the number of active monthly developers on Ethereum increased more than five-fold from 1,084 to 5,819 and the number of developers on Solana, Polkadot, Cosmos and Polygon had each grown from fewer than 200 to more than 1,000.[19]

A broadening digital ecosystem

L1 blockchains, while effective, have demonstrated some shortcomings in terms of their throughput of transactions. The time it takes to verify enough transactions to fill up a block and to go through the consensus protocol to affirm that block and add it to the chain is slow relative to the number of trades that can be processed in the centralized economy. Transactions often get backed up, and processing costs get pushed up through competition to move to the front of the queue. Indeed, Vitalik Buterin calls this the "scalability trilemma."[20] Simply put, this refers to the difficulty in achieving decentralization, scalability and security in a node-based verification system. To address this challenge, new layer 2 (L2) solutions were developed.

Layer 2 (L2) solutions

The layer 2 (L2) solution for the Bitcoin payment network was developed by Lightning Labs and is referred to as the Lightning network. This network allows two transactors to open a channel with each other by depositing bitcoin and "invoicing" each other. The two nodes

can continue to send invoices back and forth so long as the channel is open. When it is closed—by withdrawing the bitcoin—all of the associated transactions are compressed and reported to the Bitcoin network to be transcribed into the ledger.

Different types of L2 solutions have been built for the Ethereum and other L1 networks. These L2 protocols are built independently and often issue their own native payment token but rely on the associated L1 Ethereum blockchain—often referred to as the mainnet—for security and recording transactions. These types of L2 solutions utilize the same coding language, templates and primitives as the L1 blockchain but process transactions differently, typically through a process to "roll up" a whole set of transactions into a single packet that is then transmitted to the mainnet. The goal is to allow for more rapid verification of trades and lower processing costs. There are two different types of rollups being used by L2 solutions that are EVM compatible with Ethereum, the largest L1 blockchain:

- *Optimistic rollups:* These solutions accumulate a set of trades and assume that all are valid, only running a "fault proof" when they suspect that an invalid transaction may be present. Because they must wait for potential fraud challenges, it can often take significant time to post these transactions to the mainnet. Optimistic rollups look at and transmit all data in a transaction, just like verifiers on the mainnet. As such, this approach is seen as offering greater security, particularly for transactions that require minimum additional on-chain actions.[21]
- *Zero-knowledge (zk) rollups:* These solutions take a different approach, using "validity proofs" to compute transactions off-chain, looking at only key data fields. This results in much faster processing times as hundreds of transactions can be compressed before being posted to the mainnet. As such, the transfers of cryptocurrency payments from the L2 to the L1 blockchain occur more quickly, making this approach more suitable for decentralized finance.[22]

Both L2 approaches result in improved scalability that comes from more efficient processing and from the reduction in workload for the L1 blockchain, which can devote more of its capacity to the fundamental functions of security and transactional certainty. Indeed, many are likening the L2 scaling solutions to a direct-to-consumer layer and differentiating that from the mainnets that are looking increasingly like a direct-to-business offering.

Top L2 protocols include Polygon (MATIC), with a market capitalization of $8 billion as of May 10, 2023; Arbitrum (ARB), with a market capitalization of $1.5 billion; and Optimism (OP), with a market capitalization of $527 million.[23]

Sidechains

Sidechains are a hybrid between the L1 and L2 solution. Unlike the L2 solutions discussed above, sidechains have their own consensus mechanisms and maintain their own blockchain ledger, but they can share transactional details with a mainnet via a two-way bridge. These offerings are becoming increasingly popular for use cases where there is a desire for some centralized oversight, such as restricting the participants able to join into the chain or requiring full Know your customer/anti–money laundering (KYC/AML) for participants.

Though sidechains operate almost like private blockchains, they utilize the same scripting language and templates as the mainnet. As such, they can build and deploy compatible apps, but offer more control or oversight.

For the Ethereum network, the top sidechains were Gnosis (GNO), with a market capitalization of $292 million as of May 10, 2023, and SKALE (SKL), with a market capitalization of $144 million.[24]

Cross-chain bridges

The growing set of L1 and L2 solutions are creating a challenge within the crypto ecosystem. According to one article, there are more than 125 such offerings with more launches in the pipeline.[25] Each of these solutions offer slightly different opportunities and tradeoffs, but there is fragmentation in terms of their programming languages, compatibility, and interoperability. Except for instances where there is a direct relationship between an L1 and L2 blockchain or sidechain, blockchains operate like silos and are unable to communicate with each other. For example, you cannot use bitcoin on the Ethereum network nor can you use ether on the Bitcoin network.

One solution to this problem has been the development of cross-chain or multi-chain protocols that facilitate communication between different blockchains. These cross-chain solutions connect independent blockchains and enable the transfer of assets and information between them.

Most use a "lock and mint" model. Basically, they lock the tokens of one blockchain up in a smart contract (token A) and mint an equivalent value of a second chain's token (token B) which they then deposit into the user's wallet for them to use. This allows the user to avoid going to a centralized exchange or automated market maker to exchange one token for another. When the user wants to retrieve token A, they submit any unused portions of token B and those tokens are burned.

Basically, cross-chain bridges wrap a token in a smart contract and issue native tokens that can be used on another chain. This increases the interoperability of different chains and helps expand the potential of the crypto ecosystem. At the same time, however, these bridges are currently some of the most attractive points for bad actors to target due to the complexity of their operation. The security protocols for these bridges are still being developed, and it remains to be seen whether they will become a permanent part of the ecosystem.

Oracle networks

Another service built to facilitate activity in the crypto ecosystem has already become a key part of the emerging infrastructure. As the array of L1, L2, and sidechains grow and the number of applications being built on these platforms multiply, there is a corresponding need for external data to sometimes be delivered into the smart contracts being deployed on these chains.

The "if-then" clauses set out in smart contracts often require specific types of data to be submitted to determine when an action should be initiated. For example, a smart contract that has been set up to pay interest on the 15th of each month to a lender needs a recognized source of calendar information to affirm when the date turns over from the 14th to the 15th. In centralized systems, this data is often purchased, and feeds integrated into relevant applications, but this solution does not lend itself to the crypto domain.

Instead, a new type of service called an "oracle" has been developed. Blockchain oracles "are responsible for sending, executing, and verifying data obtained from external centralized sources before submitting that data to smart contracts."[26] Basically, blockchain oracles are third-party apps that bridge the gap between smart contracts and the external world.

There are two types of blockchain oracles: "software-based oracles rely on data from online sources, while hardware-based oracles rely on data from physical devices such as RFID sensors."[27]

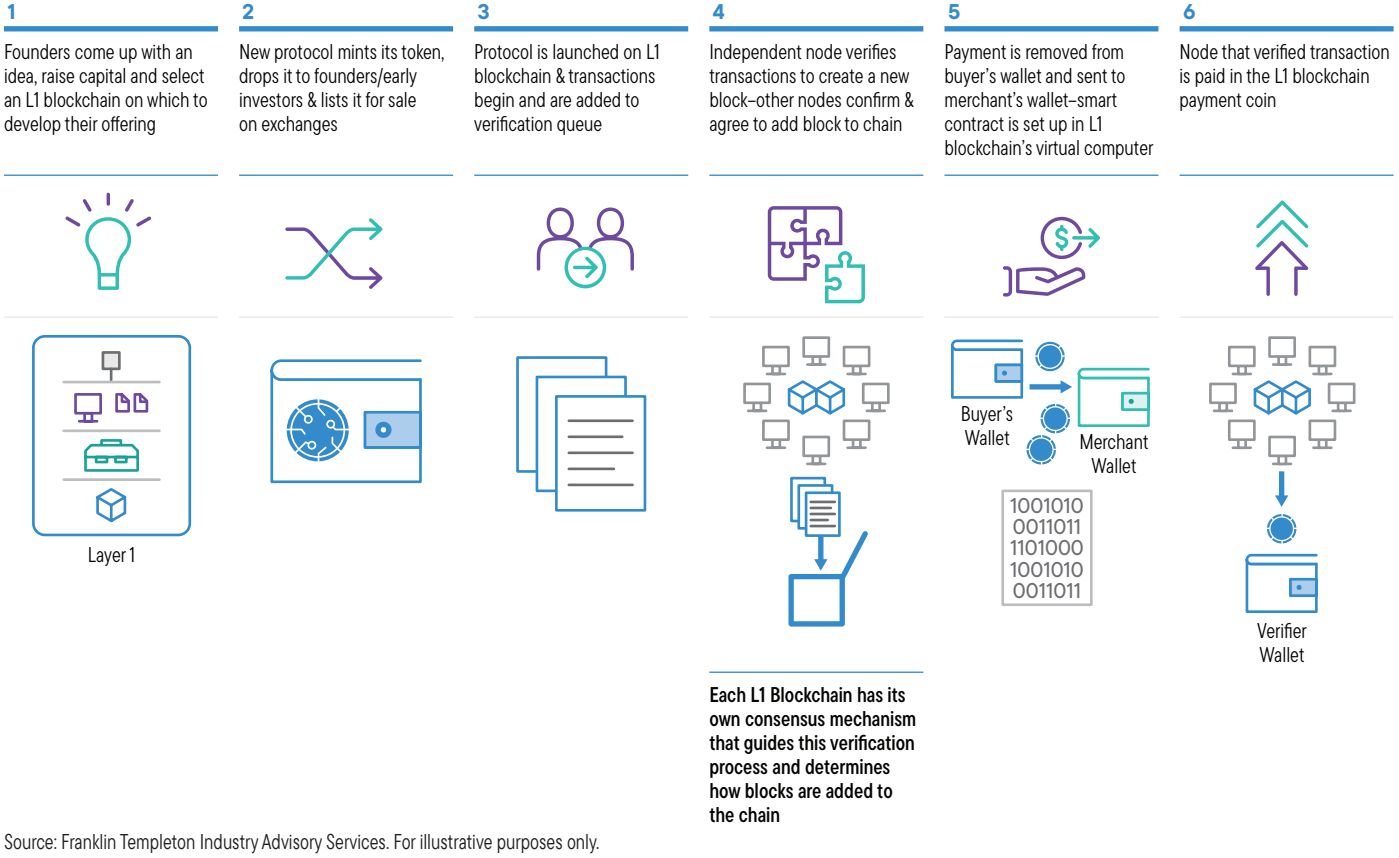
Chainlink (LINK) is the largest blockchain oracle at present, with a market capitalization of $3.4 billion as of May 10, 2023, and a 24-hour trading volume of $181 million.[28] Chainlink launched on the Ethereum network in 2019 but has since expanded its on-chain services to various other blockchains and apps. Other leading oracles include the Band Protocol (BAND) and the Decentralized Information Asset (DIA).

Having now laid out the evolution and current state of the crypto ecosystem, we will next turn our attention to showing how the pieces come together and how individuals build and operate a business on an L1 blockchain.

Building and operating a business on a blockchain

Building and operating a business on an L1 blockchain is very different from in the traditional world. Capital raising, operations, payments and governance are all different in a blockchain world, as illustrated in Exhibit 5.

Exhibit 5: Building a Web3 Business on an L1 Blockchain



Source: Franklin Templeton Industry Advisory Services. For illustrative purposes only.

Capital raising

In traditional venture capital, new projects are funded and the early investors as well as the founders are given equity shares in the new company. Often, a portion of these shares are held aside to be awarded to future employees. These shares are typically held until some type of exit is engineered from the venture, such as an initial public offering or a private share tender. For blockchain-based ventures, this process works somewhat differently.

New projects typically mint their own token when nearing launch and award those tokens to their founders and venture investors. They also tend to reserve not only a pool of tokens for their future employees, but for the "community" that they are looking to develop to build network effects for their venture. Tokens are distributed by being "dropped" into the digital cryptocurrency wallets of the founders and investors. Undistributed tokens are typically held in the foundation's account that is established to oversee the new venture.

Lockup periods are often shorter than in traditional venture investing, and the venture capital fund manager must have an ability to monetize their investment through the management of their token pool.

Operations

Businesses built on L1 blockchains are locked into their chosen ecosystem for both the contracts they use to manage their tokens and deliver their commercial value as well as for their ability to record transactions, receive proceeds, and manage the terms of engagement as laid out in smart contracts. Businesses built on a blockchain perform and operate all their functions within that ecosystem, from issuing tokens and providing services to verifying transactions and making and receiving payments.

Choosing the right blockchain on which to build a venture requires founders to consider several variables from the type of consensus mechanism used to verify trades, to the breadth of the developer community associated with that blockchain, to the security features it offers, to the speed of its transaction verification layer. Increasingly, certain blockchains are becoming associated with certain types of use cases, such as gaming or decentralized finance. Identifying one's desired community and finding a blockchain where those types of users are most likely to congregate is another important consideration.

Another facet of the crypto ecosystem gaining increased attention is the effectiveness of the user interface that can be deployed on a blockchain. Most of today's offerings have focused on the "pipes and plumbing" aspects of how the ecosystem works. Little attention has been given to the engagement layer—a goal that some of the emerging L2 blockchains are beginning to address. Many of the presentation layers offered by decentralized apps fall well short of similar Web2 apps offered in today's app stores. This makes for a somewhat difficult customer experience.

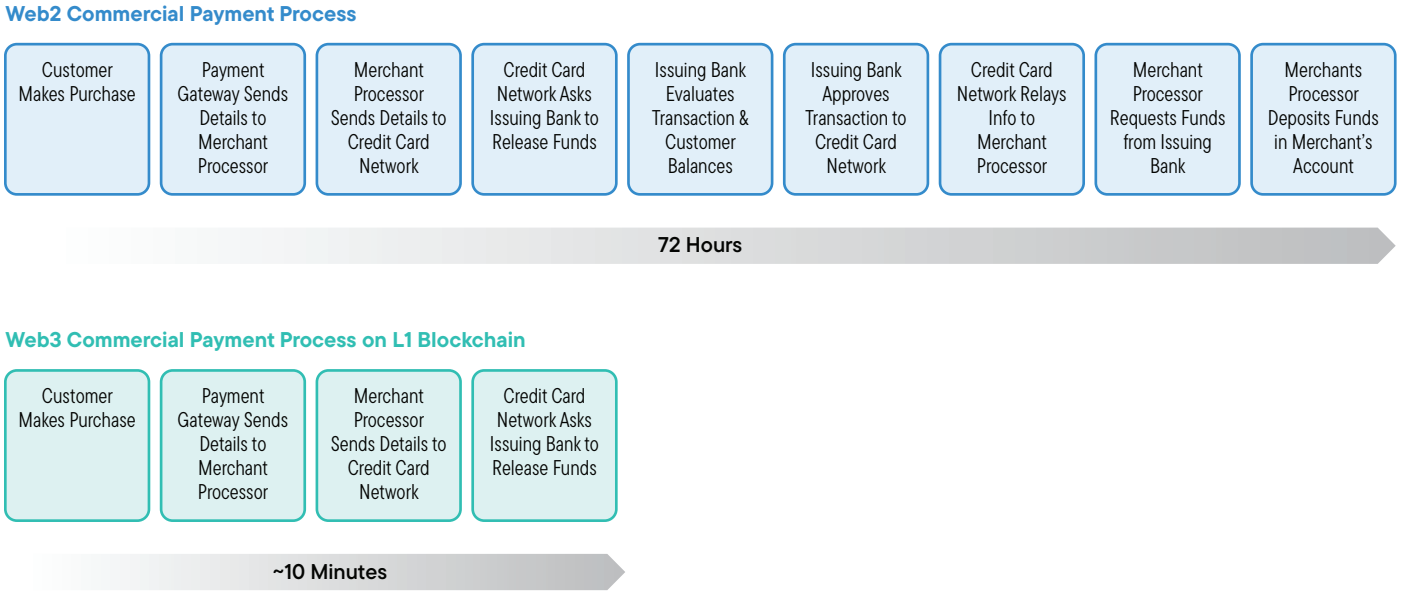
One place where the experience is far superior, however, is in the speed and certainty of payments. Indeed, once understood, it becomes clear why so many proponents of Web3 see the digital asset ecosystem as a substantial improvement over today's processes as the former is able to radically improve the speed, cost and transparency of the payment processes.

Payments in Web3

Today's payment ecosystem consists of a proliferation of intermediaries and separate transaction verification and processing companies whose entire purpose is to facilitate payments. These include brand name providers such as PayPal, Square, Visa, Mastercard, and global commercial banks such as JPMorgan Chase, Citigroup and HSBC. A whole series of handoffs, reconciliations, interfaces, confirmations, approvals, messages, lags, and checks are required in today's payment ecosystem for transactions to occur. This adds considerable cost and friction to the simplest exchange. On average, it takes about 72 hours for the money paid by a transactor to show up in a merchant's account.

The L1 blockchain's approach of incorporating transaction verification and processing into the same platform on which transactions are taking place removes the needs for many of these steps. This results in tremendous savings of both time and cost. Instant movement of payment upon verification of the transaction and the confirmation of sufficient funds in the wallet with no intermediaries or handoffs means a much shorter, faster, cheaper, and tighter chain. Even the Bitcoin network, often considered among the slowest blockchains, can move payments from the buyer to the seller in about 10 minutes. This contrast is illustrated in Exhibit 6.

Exhibit 6: Comparison of Web2 Commercial Payments versus Web3 Payments



Source: Franklin Templeton Industry Advisory Services. For illustrative purposes only.

Governance

The crypto ecosystem is being designed to operate in a decentralized rather than centralized manner. This presents a significant challenge around how to make strategic decisions about the evolution of the associated platforms and apps. Technical points from what types of upgrades should occur and when new releases should be scheduled need to be decided. Operational points such as determining a marketing and human relations budget need to be determined. People-related issues such as what to pay new employees and what new talent is required to enable the platform to scale must be agreed upon.

Early in a project's development, there is often a small group of individuals that will collectively take responsibility for the emerging project by creating a foundation to oversee the venture. This foundation collectively makes many of the early decisions, acting like an advisory board. As the venture grows, many of the tokens reserved for the "community" begin to be distributed. These tokens are often provided to those participants that bring liquidity into a venture and enable its network effects to grow. Users receive rewards via a token drop, incentivizing them to remain active and express their views about the venture's development via social channels and community chats.

When the community reaches a sufficient size, a more formal model to enable decision-making is introduced. This governance model creates a decentralized autonomous organization (DAO). DAOs typically create a new governance token that entitles holders to vote on matters of strategic importance. Governance tokens can be earned through community participation or bought by those looking to have a voice.

Formal proposals are put forward to the DAO through a structured submission process. Anyone looking to make a proposal can do so by following the rules set out by the DAO. A comment period then ensues during which members of the DAO can debate the proposal. A vote is then held. If a proposal is approved by 51% or more of the voting population, the proposal is adopted. If the proposal fails to achieve a 51% majority, it is rejected.

This is a completely new way of looking to manage a growing venture and one that will be closely monitored over the coming years to determine whether the approach can result in a long-term solution as the ecosystem evolves.

Having laid out the basics of how a business operates in the crypto domain, we will turn our attention to the nuances to consider for those looking to invest in the token-based ecosystems

Investing in crypto businesses

Investing in Web3 crypto enterprises is very different from investing in traditional businesses.

How crypto ventures differ from traditional businesses

The process of deciding whether to invest in the equity of a traditional company is well understood with the variables having been examined over many decades and many educational courses designed to inform those looking to build their own model. The inputs used to analyze the company look at the fundamentals of its business, its prospects, its competitors, its management, and its market opportunity. Analysis is also done around the company's financial position—balance sheet, income and operating statements. If the fundamental premise looks promising and the financial model shows the present value of the business's estimated cash flows as below the current market price, then the equity is considered a good opportunity and the investor will purchase and hold the equity in the hopes that it reaches the expected price target.

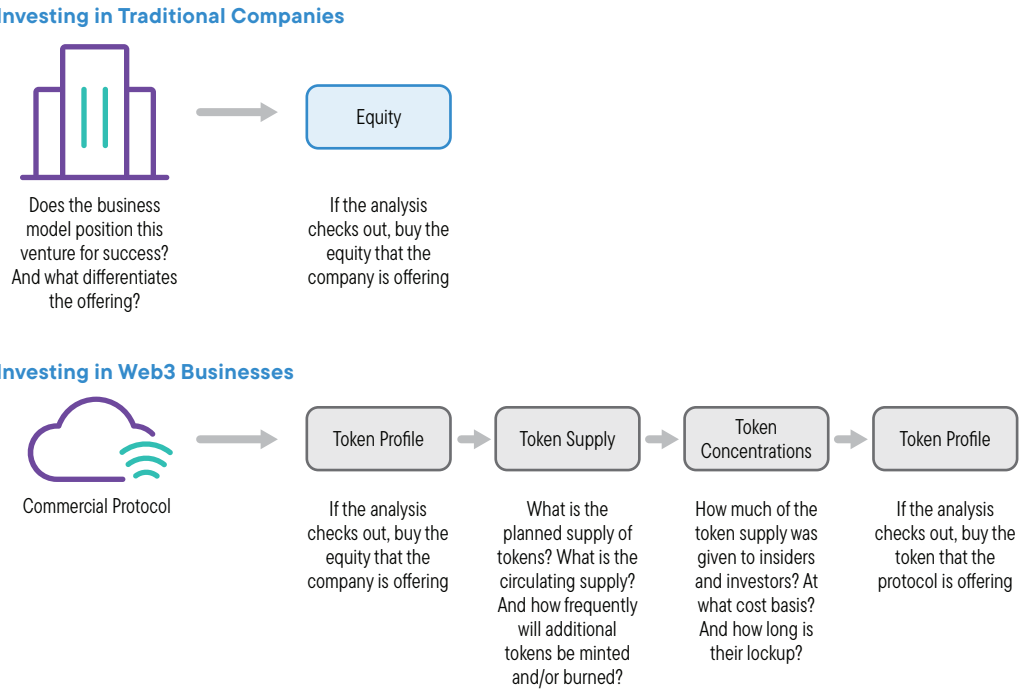
Making this same type of investment decision is considerably more complex in the crypto domain. Above and beyond the assessment of the business opportunity, there are several unfamiliar dynamics and entirely new considerations that must be evaluated and actively managed.

Even at the most fundamental level, there are important differences.

- Crypto ventures are not companies, and they do not have a dedicated management team. They are decentralized protocols comprised of a self-executing code, overseen by a foundation or a DAO, and reliant on an engaged community of users to generate network effects.
- Crypto ventures are built using processes designed as open source code and run on blockchains that provide complete transparency into the underlying transactional data. This is a significant departure from traditional businesses that own their code, extract value from proprietary processes, and utilize their transactional and customer data to generate advertising and other sources of income.
- Crypto ventures are part of a token-based economy and can issue their own proprietary tokens, but only certain types of tokens reflect the value of the underlying enterprise. This is different from an equity share that always reflects the value of the underlying company.
- Equities are registered securities. Regulators have set out stringent guidelines around such securities, and issuers must comply with certain standards of operations and disclosure. Tokens are privately issued instruments. There are no regulations at present that determine how a token offering must be administered and no guidelines on how communications about the token pool must be handled.

Investing in the crypto domain thus requires a much broader set of analyses. This is illustrated in Exhibit 7.

Exhibit 7: Considerations for Investing in Traditional Companies Versus Investing in Web3 Businesses



Source: Franklin Templeton Industry Advisory Services. For illustrative purposes only.

Determining the token-to-business relationship

As discussed in the Building Blocks section of this primer, different tokens have different functions. All token valuations can be driven up in a speculative wave, but that does not mean that such valuations are warranted. The first question an investor must ask, therefore, is whether the token will entitle the holder to benefit from the underlying protocol's success, and if so, whether the token provides a direct or derivative benefit.

A utility token such as LINK from the Chainlink blockchain oracle app entitles the holder to a service. App developers that want to have external data delivered into their smart contract must purchase the LINK token to pay the Chainlink protocol for its services. The value of the LINK token reflects demand for Chainlink services, not the value of the Chainlink protocol.

The price of a service is not equivalent to the value of a business. The price of a service token may go up if demand rises, but if the network mints sufficient tokens to meet demand, there should be little noticeable increase in the price of that token, and the price of the token may even go down as the network benefits from economies of scale.

Other types of utility tokens may not even entitle the holder to a service, but rather just bestow benefits. These offer an even less direct relationship to the value of the underlying protocol. For example, the FTX token was a utility token that provided owners an ability to receive discounts for their transactions on the FTX exchange. It was a coin that bestowed benefits like a loyalty program—as if Amazon required you to buy a "Prime" coin to become an Amazon Prime member. The FTX token had value so long as there was interest in transacting on the FTX exchange, but when that exchange failed, those tokens became worthless. The fact that many other crypto-linked organizations had accepted the FTX coin as collateral for loans was what caused the systemic risk and fallout across the ecosystem.

Besides utility tokens, other types of tokens also offer at best derivative value—a mirror of the underlying business's strength rather than an ownership interest in the business. Payment coins are meant to facilitate transactional activity. Demand for such coins may be linked to growing volumes on the underlying network, but owning the coin does not give the holder any direct benefit from the network's growth. Indeed, if the cost of the token goes up too much, it may retard network growth as was evident with ether and the Ethereum network in 2021.

Other types of tokens offer no actual or derivative value relative to the underlying business. Stablecoins, if they are operated properly, should have a steady value and neither appreciate nor depreciate in price. They offer no rights to participate in the profits that the stablecoin operator is generating through their management of the collateral pool. Governance tokens allow users to help shape a protocol and make strategic decisions but offer no financial incentive that would reflect the value of that offering. Meme coins such as Doge coin or Shiba Inu can often attract large and enthusiastic sets of investors, but there is no actual business model underlying the token. Asset-linked tokens reflect the value of a specific item, not an underlying business.

Even investment tokens that directly bestow ownership in a venture may have different and variable relationships to the commercial reality of the protocol's business.

Understanding the tokenomics of an offering

The second question a prospective investor must ask about a Web3 crypto business relates to the mechanics of its token pool. This is often referred to as the protocol's "tokenomics." Tokenomics informs the timing of an investment opportunity and highlights short-term influences that may affect token pricing. There are several considerations and new data points that an investor must consider.

The first data point an investor should examine is the *supply of tokens*. Because token issuance is driven by code, there's typically a schedule around how the supply will change over time, and this schedule can be evaluated and modeled. There are three key supply measures to consider:

- *Circulating supply:* The current supply of tokens issued and in circulation.
- *Total supply:* The total number of tokens minted to date, regardless of whether those tokens are in circulation or locked up, less any tokens that have been burned.
- *Maximum supply:* The maximum number of tokens that will ever be created.

Comparing circulating supply with total supply can inform investors about the size of the token pool that is locked up with early founders and investors. This is a concern because these holders are prevented from trading their tokens until their lockup expires. If there is a high percentage of tokens in lockup, a significant supply might enter the market all at once when the lockup expires and affect pricing.

Looking at total supply versus maximum supply informs investors about the longer-term profile of the token pool. If the total supply remains far short of the maximum supply, that might be viewed as a negative factor since there will be a lot more issuance to come to market over time. If the total supply is nearing the maximum supply, that might be viewed as a positive consideration. Some protocols opt not to set a maximum supply, which adds uncertainty to any evaluation of the protocol and its token pool.

Calculating the market capitalization of a token also requires an understanding of which supply measure is being used. Market capitalization is calculated by multiplying the token price by the token supply. If that calculation is done using circulating supply, a misleading figure may result. Looking at the fully diluted market capitalization (maximum supply multiplied by the current price) and comparing that to the circulating supply market capitalization can be another way of evaluating the token pool. For example, if the circulating supply is only half of the maximum supply, the price of the token would need to double in the long term to maintain the same market capitalization.

The second data point that an investor should consider around the token pool is the *emission schedule*. There is a programmatic element to how, when and to whom tokens are released. The journey of how today's token supply becomes the future supply is encapsulated within the token's emission schedule.

For example, some tokens may have a daily release schedule that is pre-programmed into the code. Regardless of whether there is demand for that token, more supply will be issued each day. Other tokens may have periodic release windows during which market participants can anticipate a large release of new tokens entering the circulating supply. This can act as a drag on pricing as that date approaches and cause a short-term divergence between the value of the token and its ability to reflect the value of the underlying protocol.

The final tokenomic factor to monitor is the *structural allocation* of the token supply. Initial token distribution typically takes place in two rounds—first a private sale to raise capital and then a public sale (or air drop) when a project is ready to launch.

The allocation of the ownership pool is typically spread across several constituents—founders and insiders, the foundation's treasury, early investors, a set-aside earmarked for the community, and a sleeve of tokens reserved for the public. Ideally, the token allocations are relatively balanced across these different audiences.

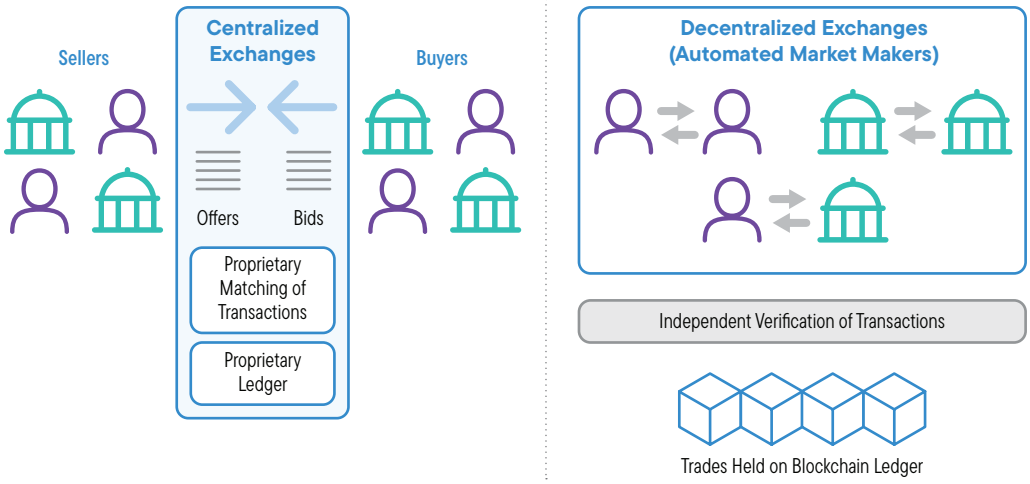
During a private sale, insiders and investors may often receive tokens at a significant discount to the eventual public issuance price and thus have an extremely low cost basis. Knowing how much of the envisioned token pool is going to these recipients is an important consideration. The vesting schedule for tokens is typically shorter than for traditional securities, and the expiration of the lockup is often known well ahead of time and tracked by the market. An overly large allocation to investors may result in significant pressure on the token price when their lockup ends. Conversely, if insiders retain too large a percentage of the token sale, it creates a higher risk for potential manipulation—like a sudden dump or an unnatural pump in supply.

As the public sale or air drop approaches, signals that too few tokens have been reserved for the community may raise concerns about the ability of the protocol to build its network effects. Similarly, preserving too few tokens for the public could make it difficult for investors to access the token pool.

Buying and selling tokens

Once a prospective investor identifies the token that they would like to buy, they need to decide where to purchase that token. While there are instances where a token is air-dropped directly into the wallet of a founder, seed investor or participant, the only option for those looking to invest in a token is to purchase that token on an exchange. There are both centralized and decentralized exchanges that facilitate the trading of listed tokens as illustrated in Exhibit 8.

Exhibit 8: Options on Where to Invest in Tokens—Centralized and Decentralized Exchanges



Source: Franklin Templeton Industry Advisory Services. For illustrative purposes only.

Centralized exchanges are traditional companies. They have a management team empowered to make their own strategic decisions. They operate their own proprietary systems and technology. They verify their own trades and typically keep their transaction records on private ledgers. They operate their platforms to maximize the potential profit for their founders, investors and shareholders. There are both publicly traded and privately owned centralized exchanges that specialize in crypto tokens.

In some jurisdictions, centralized crypto exchanges are required to register with the regulators and obtain specific licenses to be able to operate. In other jurisdictions, there are at present no rules that bind these organizations.

Centralized exchanges provide numerous services that make it easy to use their platforms. For investors unfamiliar with the mechanics of the crypto domain or uncomfortable holding their own assets, centralized exchanges can provide a digital cryptocurrency wallet and manage custody of the assets on the client's behalf. If they provide this service, the centralized exchange is supposed to keep customers' assets strictly segregated from the company's own assets.

The issue, however, is that the exchange itself runs the control and compliance processes to administer and oversee these accounts. There is no official oversight of these activities, an issue that led to the demise of the FTX exchange when it became known that customer assets were purportedly being illegally utilized by the platform operators. In the wake of that blowup, several centralized exchanges are now looking at ways of showing a "proof-of-reserves" to instill customer confidence.

Decentralized exchanges work differently. Decentralized exchanges are run either by foundations or DAOs. Users must have their own digital cryptocurrency wallet to connect into a decentralized exchange. A participant looking to buy or sell a token designates their interest, and an automated market maker algorithmically matches bids and offers for specific tokens. All transactions are verified through a consensus mechanism and are listed on a public blockchain. Every node that is a part of the network has transparency into this transactional record.

Participants in a decentralized exchange can choose to become liquidity providers to that exchange. This entails contributing a pair of cryptocurrencies and locking those balances into a smart contract. The participant is then given a liquidity pool token that represents their share of that pair's liquidity pool. Transaction fees generated by activity in that pair are split and distributed to the liquidity providers, giving any participant an option to benefit from activity on the platform.

For example, a participant could contribute ether and bitcoin. Any exchange of bitcoin for ether or of ether for bitcoin would generate a fee in the bitcoin-ether liquidity pair. If a participant had contributed 2% of the total liquidity in the pair, they would receive 2% of transaction fees collected for exchanges of bitcoin and ether.

Staking and decentralized finance (DeFi) transactions

Participating in a decentralized exchange's liquidity pool is one way that investors can use their tokens to generate additional yield. Other ways to leverage tokens for financial gain are also being developed.

Proof-of-stake networks provide a pathway for a broader set of participants to earn rewards without having to directly perform any verification activities. Participants can pledge capital to a staking pool. These pools are offered by some validators in order to create a larger stake and thus position their node for more opportunities to verify blocks and earn rewards.

The validator in this scenario would earn a commission for verifying the block, and the reward would be paid directly by the blockchain to members of the staking pool based on their proportionate contribution to the pool. This is a new way of earning yield on a deposit that is meant to help owners of the blockchain's currency offset inflationary impacts. As the number of transactions on a chain increases, more coins are minted. Without the reward, this increase in the token supply would be inflationary for long-term coin holders. The reward size is set to help offset such inflationary pressure.

Specialized apps are also being developed within the blockchain ecosystem to enable participants to pursue other types of financial use cases.

Lending apps allow individual participants to lend or borrow tokens. Users can loan their tokens to a lending pool and receive an interest payment proportionate to their share of the overall pool. Borrowers can withdraw tokens from a lending pool and pay interest into the pool for the duration of their transaction.

Lenders are issued a new token from the lending app that represents the value of the tokens they contributed into the pool and specifies the share of the interest payment that they will be entitled to receive. This new token can be held by the lender in their wallet as a claim against the supply they provided and the interest payments or it can be circulated within the crypto ecosystem and be sold to another participant.

If the coin is sold, the right to redeem the tokens and collect the proportionate share of the lending pool's interest payments transfers to the new holder. For instance, certain stablecoin providers accept cryptocurrency tokens into their collateral pool. A holder could pledge their lending app token and receive an equivalent supply of stablecoins if they so desired. The stablecoin provider would then become the new owner of the lending app token and be entitled to both the tokens in the lending pool and the interest payments.

Whoever holds the lending app token—whether the original lender or another participant that took subsequent possession of the token—can unwind the loan and receive back the original pledge of tokens or coins whenever they desire by submitting the lending app coin back to the lending app. At that time, the lending app token would be burned, and the designated number of tokens sent to the submitter's wallet address.

Leading lending apps include Aave (AAVE), with a $934 million market capitalization and $48 million 24-hour trading volume as of May 10, 2023, and Compound (COMP), with a $273 million market capitalization and a $17 million 24-hour trading volume.[29]

It should be noted, however, that each of these activities—pledging to a liquidity pool, joining a staking pool, lending tokens and borrowing tokens—still sits outside the regulatory perimeter. There are no investor protections to guarantee the safety and soundness of these transactions and there is no guarantee that regulators may not decide to restrict or prohibit such activities in the future.

Yet, as this section highlights, the Web3 digital asset ecosystem is actively exploring new ways for participants to be able to direct and extend their own investment-related activities in the emerging ecosystem. Options discussed this far, however, all deal with fungible tokens. This category includes cryptocurrencies issued by payment networks, stablecoins, or native tokens issued by decentralized applications. Asset-linked tokens are typically issued in a different, non-fungible format. Specialized marketplaces deal with the exchange of these types of tokens, offering yet another pathway for investors to participate.

Non-fungible tokens

Implicit in the preceding discussion of tokens was the assumption that one token is substitutable for another, in the same way that every bond in an issue is identical and therefore interchangeable. Bonds are said to be *fungible*. By contrast, a painting is not. Vincent van Gogh's *Sunflowers* is unique and can't be substituted for Leonardo da Vinci's *Mona Lisa*, or vice versa. A painting is non-fungible. In the same way, some tokens are fungible—identical and substitutable—and others representing unique assets are *non-fungible*.

Non-fungible tokens are known as NFTs. As of May 10, 2023, $56.4 billion worth of NFTs have been sold in over 179 million transactions to almost 11 million buyers.[30] NFTs are frequently in the news in connection with the world of art and collectibles, where unique assets are the norm. For example, Mike Winkelmann—or Beeple as he is better known—an American graphic designer and world-famous digital artist, sold his first NFT in February 2021, *Everydays—The First 5000 Days*, for over $69 million.[31]

This was the first piece of NFT art auctioned by Christie's; and it was the first time Christie's had accepted ether, a cryptocurrency, in payment. But such attention-grabbing headlines obscure the real, and much bigger, story. This concerns the potential that NFTs offer to expand not only the set of tradable assets, but the way that we grant ownership and utilization rights.

Embedding property rights in a token

Wrapping an asset in a token offers the prospect of widening the universe of what we think of as both investable and transferable assets. Many tangible assets (homes, vineyards, art) and digital assets (music catalogs, film and television rights) are investable, but they are not easily transferable. Each transaction requires a new set of ownership documents to be drafted, money to be wired and/or payments processed, licenses and/or titles to be transferred from the name of the seller to the name of the buyer, and more steps to finalize a sale. Different intermediaries would need to be involved at each stage, and it can often take significant time to coordinate all the required steps and handoffs.

Beyond the operational frictions of transferring assets, there are also challenges in obtaining and administering the financial rewards associated with these assets. Income-generating assets require teams of people to collect, apportion, and distribute proceeds. Assets that appreciate require appraisals and intermittent valuations from third parties. As a result, the amount of work that is required to administer these assets not only limits their transferability, but it also limits the number and velocity of such transactions, particularly for individual investors that must navigate these hurdles on their own.

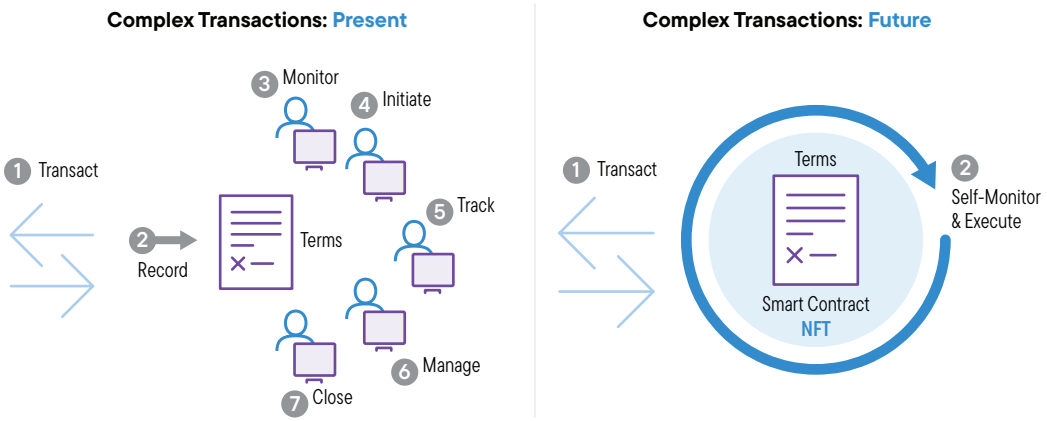
Other physical assets such as collectibles (trading cards, sneakers, dolls) are tradable, but it is hard to make them investable. Transactions are typically done bilaterally between enthusiasts or between specialized distributors and a single buyer. Verifying the authenticity

of an item, evaluating its condition, and controlling its physical location are all challenges that make it hard to bundle these assets into portfolios and allow a pool of potential investors to benefit from the appreciation of value in these items.

Finally, there is a whole range of intangible assets that have value and offer new sources of income and/or appreciation that are neither investable nor tradable today. Consider the huge amount of value locked in the creator economy where only the most successful influencers earn income and, even then, the payouts they receive are entirely decided by and heavily skewed in favor of the sponsoring platforms. Or consider the gaming ecosystem, where monies are constantly being directed to the purchase of in-game assets, but where there is no mechanism to exchange or extract that value. Finally consider the intangible assets being created by leading enterprises—data, algorithms, patents, loyalty programs—where there is no ascribed value given to these assets and there is no way to directly invest in these resources—only in the equity of the entire company.

Tokenizing these assets by embedding the asset itself (if digital) and/or by embedding a smart contract to bestow the ownership rights and title to an asset offers a way to improve the utility of these offerings by making them both investable and transferable as shown in Exhibit 9.

Exhibit 9: Simplifying the Delivery of Complex Transactions with an NFT



Source: Franklin Templeton Industry Advisory Services. For illustrative purposes only.

Non-fungible tokenized assets can be tracked on a blockchain. The digital wallets holding these assets can be readily identified. When an NFT is sold, the ownership record is automatically transferred from the seller to the buyer by the blockchain and the change in state recorded in the blockchain's virtual computer. Asset-related processes such as the distribution of income can be automated and administered via smart contracts. External data such as valuations or sales figures can be delivered into the smart contract from blockchain oracles to help inform the asset's worth.

Tokenization should thus enable more of these types of assets to become part of investor portfolios in the future, helping to diversify the sources of investment value. The token structure, however, also enables something completely new. The smart contracts embedded in an NFT can bestow more rights beyond property rights since they are programmable and self-executing. NFTs can bestow non-financial rights such as privileges, access, and utility. These rights make the purchase of an NFT about more than its financial value. Indeed, NFTs offer a way to deliver an experience to the holder.

Delivering experiences via an NFT

The programmability of a smart contract embedded in an NFT enables these offerings to deliver an infinite number of features, enabling their owners to do and experience things in both the physical and in the digital world. Rights to access communities, conferences, events, locations, transportation, exclusive content and more can be embedded in an NFT. Rights to utilize the asset to obtain discounts, incentives, previews and benefits can be embedded. NFT holders can be elevated to receive special products or engage with celebrities or public figures in unique ways or obtain privileges that offer them status and prestige. Moreover, these rights, just like the ownership rights, are easily transferrable via the blockchain ecosystem.

This will support new business models and disrupt existing ways of doing business. By issuing tickets as NFTs, venues could give a variety of benefits directly to certain purchasers such as discounts on merchandise and concessions or access to a commemorative collectible from that day's event. Moreover, the data generated by the NFT use could be harvested and used to improve the sponsoring business's customer targeting and economic outcomes. For example, Walt Disney World's MagicBand is an off-chain equivalent of an NFT that transformed the organization's business model, enabling individual experience customization and revenue optimization to a degree that was unthinkable previously.

NFTs also offer businesses a way to blur the lines between their physical and digital offerings and individuals a way to bridge their physical and digital lives. As an article published in the Harvard Business Review puts it, "owning an NFT effectively makes you an investor, a member of a club, a brand shareholder, and a participant in the loyalty program all at once."[32]

NFTs thus offer a transactional gateway for companies to build and cultivate a community around their brands, create high-value interactions, blend their digital and physical offerings, and connect cohorts of individuals into niche networks. NFTs are both a way of delivering a transaction and a vehicle through which they can engage the client. They augment a basic purchase and create a more valuable "experience," which in turn allows for a richer and stickier pre-and post-transaction relationship between the provider and the consumer.

NFTs also offer new opportunities for individuals. Today, many creators miss out on a lot of the financial benefit of their art. Creators may receive a direct payout when they sell the rights to their work, but they are unable to benefit from future sales and the ongoing appreciation of their creations. A smart contract can be embedded into an NFT that entitles the original creator to a percentage of the initial and all subsequent sales of that work, allowing them to benefit from any future increase in value. Customers create valuable data trails based on their interactions and transactions, but they are unable to reap any of the financial benefits that many organizations obtain by utilizing (and often selling) their data. In the future, individuals may be able to mint an NFT to control access to their data and demand financial compensation for its use.

The various types of NFTs, rights they bestow and return characteristics are highlighted in Exhibit 10 on the next page.

NFT marketplaces

Specialized marketplaces are emerging in the Web3 ecosystem to facilitate the minting, issuance, sale and exchange of NFTs. For now, these marketplaces are only enabling participants to create offerings around digital assets. Unique pieces of digital art such as the one featured in the Beeple sale noted earlier can be uploaded and structured as an

Exhibit 10: Opportunities to Create a Range of Investable and Transferrable NFTs

Smart Contract Rights	New Options for Ownership	Examples of Tokenized Assets	Return Characteristics
Property Rights		• Property–home equity, stadiums, resorts • Private Businesses–vineyards, farms, sports teams • Infrastructure–pipelines, bridges, toll roads • Personal Assets–data, collectibles, cars	• Share of revenues • Share of appreciation • Share of sales value
Intellectual Property Rights		• Video, film, television, theater projects • Paintings, sculpture, photography, fashion • Songs, recordings, books, blogs, podcasts • Patents, algorithms, models, code	• Share of copyright payments • Share of royalty pools • Share of sales & resale value • Proof of provenance
Utilization Rights		• Exclusive access–shows, conferences, communities • Exclusive experiences–lessons, excursions • Exclusive benefits–discounts, upgrades, offers • Elevated priority–product releases, service queues	• Prestige • Reward • Buying power • Convenience

Source: Franklin Templeton Industry Advisory Services. For illustrative purposes only.

NFT using these marketplaces. Platforms make the user experience of minting an NFT as easy as uploading photos or video to a social media site. The smart contract template is set up, and users need only populate their information and terms. They can then issue these NFTs for sale directly on the platform.

Top NFT marketplaces at present include Blur, with a transaction volume of $677.9 million over the prior 30 days as of May 10, 2023, and OpenSea, with a 30-day transaction volume equivalent to $236.5 million.[33]

Collections of limited edition NFTs are also offered. These collections are typically created by a professional organization and released as a series. They use a piece of digital art as a cover and then provide a broader set of privileges to the holder via an embedded smart contract that they program themselves. Popular series such as the Bored Ape Yacht Club offer access to an exclusive community plus unique digital art configurations of the ape mascot. Other top NFT collections include CryptoPunks, NBA Top Shot, and Axie Marketplace.

Risks associated with digital assets

While the Web3 digital asset ecosystem offers tremendous potential, the space is new and constantly evolving. These should be considered frontier risk assets until the regulatory environment solidifies and vulnerabilities in business models and their operation are fully exposed and addressed. The most important risks to consider can be split into two broad categories—system-related risks and participation risks.

There are also risks in investing. The initial potential of any asset class may not carry over to any specific company or the entire asset class chosen for investment, over any time period. Any of the stated assumptions may or may not come to fruition, and any companies referenced may or may not have future successes. Investors should be prepared for potential losses as well as the possibility of investment gains. Ideas, products, companies, themes or entire asset classes with positive attributes are not indicative of future results. Discussions should not be regarded as any type of trading recommendation, or as a signal about any past, current or future trading activity in any fund or strategy, by Franklin Templeton and its affiliates.

System-related risks

- *Business model risks:* Decentralized business models are a new and novel concept. Use cases are being designed and tested in real time. Service delivery and operational activities are reliant on well-written code being deployed on new technologies. The entire ecosystem is still being vetted and evolving, and there are no central authorities able to resolve disputes or management teams to be held accountable for missteps. Financial apps, in particular, are pushing the boundaries on how to deliver new services. These offerings are often being coded by individuals with little understanding or knowledge of the financial controls that have been designed and built into offerings in the off-chain ecosystem. This can result in unexpected risks, vulnerabilities and unintended consequences.
- *Smart contract risks:* Smart contracts are an increasingly important part of the ecosystem. The code deployed in such contracts is self-executing. If the right conditions are met, the programmed actions will be undertaken. Moreover, multiple smart contracts may be triggered simultaneously which might lead to unexpected outcomes or issues. Manual interventions can sometimes be attempted after an event has occurred but may not always be successful due to the speed at which the platform operates.
- *Interoperability risks:* Activities in the ecosystem are built around the orchestrated movement of tokens. Tokens are designed to be interoperable. Apps built on the same platform can recognize and accept tokens from other apps as part of their business flow. New models such as DeFi wrap tokens from one app in new tokens and allow those new tokens to be used by other apps. This creates a number of interdependencies. While an orderly exit can be anticipated in most instances, in a crisis a sudden surge in requests to unwind positions and redeem underlying collateral may overwhelm the system and cause contagion. Failures in one app's ability to handle requests may spill over to other apps, creating a cascade that necessitates suspending activities or taking other steps to restore order across the network.
- *Security risks:* While the Web3 ecosystem has been designed to be decentralized, the risk mitigation and cybersecurity strategies being deployed to protect the networks and apps have been designed to work with centralized business models on platforms and systems that are manually supervised. Many of these tools have not been designed to operate 24 hours a day, 7 days a week, 365 days a year in an environment that relies on self-executing code. Design gaps, particularly in key infrastructure whose functionality is still being tested (such as with cross-chain bridges), can be exploited and tokens stolen before fixes are identified and deployed.
- *Reputational risks:* Perceptions about the emerging digital ecosystem are still being shaped, and confidence can be easily shaken. The pseudo-anonymous nature of public blockchains and early history of Bitcoin being used to fund illicit activity from bad actors has tainted many people's judgement about the wider ecosystem and the potential of its underlying technology. The excessive run-up and collapse of valuations due to the rapid influx and withdrawal of pandemic-related retail capital shook confidence in the ecosystem. Many institutional investors that avoided direct crypto exposure but participated via venture capital investments have seen valuations decline sharply during crypto winter. Some well-known economists, financial experts and businessmen continue to denigrate the space, questioning its value and legitimacy. Each of these considerations might slow adoption and/or influence regulators to take extreme positions that could curtail growth of the ecosystem.

Participation risks

- *Investment risks:* The ease with which investors can access the crypto ecosystem coupled with a lack of any regulatory disclosure rules or professional guidance often means that investors place money into the ecosystem with little or insufficient understanding about the investment they are making. As discussed earlier, unlike equities, not all tokens reflect the value of the businesses that issue them. The entire field of tokenomics is new, and little professional research is being provided to help investors evaluate specific opportunities. Diligence on emerging projects and token issuances is often lacking. Opportunities for fraud abound.
- *Safe-keeping risks:* Tokens are held in digital cryptocurrency wallets. Investors can self-custody their assets but run the risk that they lose their access key or storage device, making it impossible to retrieve their holdings. Third-party custody is available as an alternate solution, but the cost of having holdings insured often limits this option to institutional or professional investors. Most novice participants in the ecosystem opt for integrated custody through a centralized exchange, meaning that the exchange maintains a wallet on behalf of the investor. These centralized exchanges are not regulated, they have no mandatory disclosure rules, they execute and verify their own transactions without any independent oversight, and they typically keep a private ledger that is not blockchain-based. This creates a risk that a bad actor might access and redirect client assets—an issue that allegedly helped lead to the demise of the FTX exchange. Many centralized exchanges are beginning to offer proof-of-reserves to help diffuse such concerns, but there is no mandate that requires such disclosure.
- *Stablecoin risks:* Although stablecoin providers are supposed to hold a sufficient pool of collateral to back the full value of each coin that they mint, there are no requirements for them to report on or disclose their holdings. In the past, investigations found that certain coins were not fully collateralized at certain points in time. Moreover, many stablecoin operators opt to invest portions of their collateral pool into risk assets to generate yield for their venture. This can create liquidity risks, particularly since many of the instruments the stablecoin operators use to obtain yield are traditional securities that do not trade 24/7/365. Demand for stablecoin redemptions over a weekend or after market hours can thus result in a liquidity mismatch.
- *Regulatory risks:* At present, there is no clear, homogenous set of regulations for the crypto ecosystem. Certain governments have created or proposed regimes that would provide oversight and guidelines to help build confidence in the system, and other governments have imposed restrictions to limit or prohibit activities altogether. Many aspects of regulation are still under consideration or development. In the U.S., there is even a debate around which regulatory body has responsibility for the ecosystem. Certain activities taking place today run the risk of being curtailed or prohibited in the future. Beyond activities within the ecosystem, access points that enable participants to move fiat currency into crypto or exchange crypto assets for fiat currency may be cut off. Decisions in this regard may be applied differently in different jurisdictions.

Understanding, considering and staying abreast of both the systematic and participation risks in the Web3 digital asset space is an important responsibility for those looking to engage with these new opportunities and experiment with these new technologies. However, it is important to remember that this entire domain is less than 15 years old and that it is evolving rapidly. Innovation is exciting and important, but not without risks. Over time, the models are likely to stabilize, and the regulations will come into focus, but in the meanwhile, this is truly a space where opportunities for substantial reward are still matched by equally significant risks.

Endnotes

1. Source: "Today's Cryptocurrency Prices by Market Cap." CoinMarketCap. As of May 9, 2023.
2. Source: Flynn, Jack. "How Many Businesses Accept Bitcoin? [2023]: 21 Important Bitcoin Statistics." Zippia. June 24, 2022.
3. Source: "Today's Cryptocurrency Prices by Market Cap." CoinMarketCap. As of May 9, 2023.
4. Source: Akolkar, Bhushan. "Chainlink moved $6.9 trillion transaction value, hosted 1,600 projects and delivered more than 5.8B data points." Crypto News Flash. January 4, 2023.
5. Source: "Today's Cryptocurrency Prices by Market Cap." CoinMarketCap. As of May 9, 2023.
6. Source: Dashboard: DeFi Overview, Total Value Locked. DeFiLlama web site. As of May 15, 2023.
7. Source: NFT Marketplaces, volume (period "all"). DappRadar web site. As of May 15, 2023.
8. Source: "Blockchains With The Highest Developers Count In 2023." March 6, 2023.
9. Source: Haqshanas, Ruholamin. "Number of Devs on Solana, Polygon, Cardano & Co Growing Faster Than on Ethereum." Cryptonews. January 6, 2022.
10. Source: Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." bitcoin.org.
11. Ibid.
12. Ibid.
13. Ibid.
14. Source: Cuofano, Gennaro. "Ethereum: The History of Ethereum." FourWeekMBA. March 7, 2022.
15. Ibid.
16. Source: "NFT Marketplaces." DappRadar. As of May 9, 2023.
17. Source: "Today's Cryptocurrency Prices by Market Cap." CoinMarketCap. As of May 9, 2023.
18. Ibid.
19. Source: "2022 Electric Capital Developer Report." Electric Capital Partners web site. January 17, 2023.
20. Source: "A beginner's guide on blockchain layer-2 scaling solutions." Cointelegraph.
21. Ibid.
22. Ibid.
23. Source: "Today's Cryptocurrency Prices by Market Cap." CoinMarketCap. As of May 10, 2023.
24. Ibid.
25. Source: "What are Cross-Chain Bridges?" Alchemy. May 10, 2022.
26. Source: Weston, Georgia. "Top 10 Blockchain Oracles." 101 Blockchains. February 22, 2023.
27. Ibid.
28. Source: "Today's Cryptocurrency Prices by Market Cap." CoinMarketCap. As of May 10, 2023.
29. Ibid.
30. CryptoSlam. "Top NFT Collectible Sales." As of May 10, 2023.
31. Source: Thaddeus-Johns, Josie. "Beeple Brings Crypto to Christie's." New York Times. February 24, 2021.
32. Source: Kaczynski, Steve, and Kominers, Scott Duke. "How NFTs Create Value." Harvard Business Review web site. November 10, 2021.
33. Source: "NFT Marketplaces." DappRadar. As of May 10, 2023.

Glossary

App-issued tokens
Developers building applications on a blockchain can create tokens for a variety of purposes. There are four main types of tokens issued by decentralized apps: **utility tokens** are used to gain access to and enable consumption of a protocol's services or to bestow certain privileges; **investment tokens** represent ownership in a project or venture and can be thought of as analogous to shares of equity; **governance tokens** permit the holder to vote on issues pertaining to the app's underlying protocol, its business practices, and its strategic direction; and **asset-linked tokens** represent ownership of an underlying asset and include an embedded contract describing the specific ownership terms and utilization rights that will be provided to the token holder.

Bitcoin
Bitcoin is the largest and original blockchain. In the white paper that introduced Bitcoin, published in October 2008 by Satoshi Nakamoto, the anonymous creator(s?) of Bitcoin, the author described their vision of a peer-to-peer electronic cash system that would allow online payments to be sent directly from one party to another without having to go through a financial institution or be intermediated in any way.

Blockchain
A blockchain is a digital record or ledger of transactions, duplicated and distributed across an entire network of computer systems. Blockchains represent complete records of all transactions ever performed within that system. Every node in the blockchain network has a real-time, simultaneously updating copy of this ledger. Every node sees new blocks of transactions being appended to the existing chain of verified blocks and could re-create the entire sequential history of transactions on that chain stretching back to the very first (genesis) trade on the ledger. Blockchain is sometimes described as "distributed ledger technology" or DLT.

Blockchain oracles
Blockchain oracles are third-party applications that send, execute and verify data obtained from external centralized sources before submitting that data to smart contracts, essentially bridging the gap between smart contracts and the external world.

Consensus mechanism
A consensus mechanism is the collective work of validator nodes on a blockchain to verify the accuracy of each transaction. A "consensus" must be reached across the nodes in the network, and when achieved, the verified data is added in a new block on the blockchain. There are different types of consensus mechanisms, but the two main consensus mechanisms used are proof-of-work (PoW) and proof-of-stake (PoS).

Cryptocurrency token
A cryptocurrency or payment token (or coin) is used for payments in the Web3 digital asset economy, just as government issued fiat currencies such as the US dollar, euro or Japanese yen are used for payments in the traditional economy. Similar to nations issuing their own currency, each blockchain can issue its own cryptocurrency in the form of a token. The term cryptocurrency is used because these monies are cryptographically protected so that each token can be identified and tracked to prevent unauthorized movements and duplication.

Cryptocurrency wallet
A cryptocurrency wallet is necessary for token owners to participate in a blockchain ecosystem. This wallet is essentially a piece of software that provides an interface between the owner and the blockchain. Cryptocurrency wallets are simply addresses on the internet where assets can be stored. There is no identifying information on these wallets other than a long string of letters and numbers. Instead of containing the asset itself, the wallet contains a digital key that is required to unlock and access the holdings in the user's wallet. These keys are only shared when a user authorizes a transaction.

Decentralized applications
Decentralized applications or dApps are digital applications built and run on a blockchain instead of on a single computer. They use open-source code and operate on distributed protocols, which means users can view, audit, and verify how they work and directly engage with them without the need for access credentials and are thus outside the purview and control of a single authority. DApps can be developed for a variety of purposes including gaming, finance and social media. For example, a developer can create a Twitter-like dApp and put it on a blockchain where any user can publish messages. Once posted, no one—including the app creators—can delete the messages.

Decentralized autonomous organizations
Decentralized autonomous organizations (DAO) are web-native, self-governing entities with no central governing body. DAOs execute rules established by its member community, which shares a common goal to act in the best interest of the entity. The rules are written into the code of the organization via smart contracts, which form the basis of the DAO's self-governance. DAOs typically create a new governance token that entitles holders to vote on matters of strategic importance. Governance tokens can be earned through community participation or bought by those looking to have a voice.

Decentralized exchanges
Decentralized exchanges are run either by foundations or DAOs. Cryptocurrency holders must have their own digital cryptocurrency wallet to connect to a decentralized exchange. A participant looking to buy or sell a token designates their interest and an automated market maker algorithmically matches bids and offers for specific tokens. All transactions are verified through a consensus mechanism and are listed on a public blockchain. Every node that is a part of the network has transparency into this transactional record.

Decentralized finance
Decentralized Finance (DeFi) is an umbrella term for the global borderless financial system enabled by public blockchains. Instead of relying on centralized intermediaries like banks, stock exchanges, or brokers, DeFi services use smart contracts—self-executing software of encoded rule sets that network participants can inspect and audit for authenticity—to record transactions and transfer funds. Central authority is replaced by group consensus.

Ethereum
Ethereum, developed by Vitalik Buterin, is the second largest L1 blockchain technology that set out to build a new open-source development platform on top of a blockchain payment network where programmers could develop a whole array of applications to operate in a decentralized manner. Ethereum's native cryptocurrency is known as ether, or ETH.

Layer 1 Blockchain

Layer 1 Blockchain (L1) is the foundational layer and main structure of a blockchain network. L1's are the most basic form of blockchain, providing the infrastructure for all other applications and protocols that are built on top of the network. Bitcoin and Ethereum are examples of L1 blockchains.

Layer 2 Blockchain

Layer 2 Blockchain (L2) refers to a secondary framework or protocol that is built on top of an existing blockchain system. The L2 solution for the Bitcoin payment network was developed by Lightning Labs and is referred to as the Lightning network. This network allows two transactors to open a channel with each other by depositing bitcoin and "invoicing" each other. The two nodes can continue to send invoices back and forth so long as the channel is open. When it is closed—by withdrawing the Bitcoin—all of the associated transactions are compressed and reported to the Bitcoin network to be transcribed into the ledger. L2 protocols are built independently and often issue their own native payment token but rely on the associated L1 Ethereum blockchain—often referred to as the mainnet—for security and recording transactions.

Mining

In proof-of-work (PoW) blockchains, such as Bitcoin—the largest and original blockchain—validators, or "miners," race to solve an increasingly complex cryptographic puzzle ("mine"). The winner of this race gets to add the block to the chain and earn the block "reward" for having done so. The reward is paid in the native currency of the blockchain. The network automatically mints new currency to pay the miners. This is how the token supply, or money supply, increases in a proof-of-work blockchain.

Minting

Minting is the process of generating new coins through verification of data, creation of new blocks, and documentation of the verified information on a blockchain network via Proof-of-stake consensus mechanism. These newly minted coins are circulated in the market for trading purposes.

Node

A node is a computer or device connected to other computers or devices that run a blockchain's software to validate, store and update the complete history of transactions on the network. Nodes are integral to the blockchain, verifying data to be added to a blockchain via a group consensus mechanism with other nodes, and maintaining the integrity of the network.

Non-fungible tokens

Some tokens are fungible—identical and substitutable—and others representing unique assets are *non-fungible*. Non-Fungible Tokens (NFTs) are a unique, cryptographic unit of data that exists on a distributed ledger and cannot be replicated. They can represent digital media or real-world, tangible assets like artwork and real estate, making buying, selling, and trading more efficient, while reducing the scope for fraud. NFTs can also represent identities, property rights, or even a bundle of rights—all encoded into digital contracts or attestations.

Optimistic rollups

An optimistic rollup is an L2 solution that accumulates a set of trades and assumes that all are valid, running a "fault proof" when they suspect that an invalid transaction may be present. Because they must wait for potential fraud challenges, it can often take significant time to post these transactions to the mainnet. Optimistic rollups look at and transmit all data in a transaction, just like verifiers on the mainnet. As such, this approach is seen as offering greater security, particularly for transactions that require minimum additional on-chain actions.

Proof-of-stake

Proof-of-stake (PoS) is a consensus mechanism by which validators commit their own capital (stake) as collateral to verify transactions and mint new blocks onto the blockchain. The larger the stake, i.e., the more capital put at risk, the higher the probability of that validator being selected by the protocol to verify a new block of transactions and earn a reward for doing so successfully. In this way, those with the most to lose are most involved in the operation of the system and validators become increasingly invested in the integrity and continued operation of the system.

Proof-of-work

Proof-of-work (PoW) is the consensus mechanism through which Bitcoin and other cryptocurrencies verify new transactions before they are added in a new block to the existing blockchain. Miners race to complete a complex cryptographic puzzle, known as hash functions, to verify and add transactions to the blockchain, in order to earn a reward in the form of new coins or transaction fees.

Protocol

In computer science, protocol refers to the basic set of rules in code that allow data to be shared between computers. In the context of blockchain, protocols are rules that govern a blockchain network—the common communication rules that the network operates according to. Two key protocols are Bitcoin and Ethereum. Their respective protocols establish the structure and operation of their blockchain. Protocols are developed by teams of people such as foundations, private companies, or groups of developers who collaborate to establish rules with parameters that will create the blockchain.

Sidechains

Sidechains are a hybrid between the L1 and L2 solution. Unlike the L2 solutions discussed above, side chains have their own consensus mechanisms and maintain their own blockchain ledger, but they can share transactional details with a mainnet via a two-way bridge. These offerings are becoming increasingly popular for use cases where there is a desire for some centralized oversight, such as restricting the participants able to join into the chain or requiring full Know your customer/anti–money laundering (KYC/AML) for participants.

Smart Contracts

Smart contracts are self-executing contracts in the form of code that are housed on a blockchain. Just as a transaction is recorded on the blockchain, the terms of the transaction are also recorded on the blockchain.

Stablecoin

A stablecoin is a type of token that has its value pegged to another currency, commodity, financial instrument, or basket, and should, if well designed and operated, maintain a steady value, neither appreciating nor depreciating in price. Stablecoins typically tie their value to the US dollar in some way. The collateral pools associated with these stablecoins are primarily, though not exclusively, comprised of government-issued fiat currencies or fiat-denominated fixed income securities.

Staking

Staking is how validators who participate in Proof-of-stake earn rewards. Validators "stake" their cryptos as collateral for a period of time while they verify transactions on a blockchain. One can liken staking to depositing cash in a high-yield savings account: banks lend deposits, and the depositor earns interest on their account balance. Staking rewards are calculated in percentage yields, and returns are typically higher than interest rates offered by traditional banks.

Tokens

Tokens are used to facilitate payments, initiate services, bestow ownership, authorize voting, convey rights, and transfer assets. Specialized tokens are used for each of these functions. Broadly, these specialized tokens can be broken down into two categories: cryptocurrency tokens and app-issued tokens.

Tokenization

Tokenization is the process of converting, through symbolic representation or encoded rule sets and attestations, something of value into a digital token that can be transacted on a blockchain. These tokens can represent tangible assets like gold, real estate, and art, or intangible assets like voting rights, ownership rights, or content licensing.

Tokenomics

Tokenomics informs the timing of an investment opportunity and highlights short-term influences that may affect token pricing. Tokenomics describes the topic of understanding the supply, demand and economic characteristics of digital assets. This entails a number of considerations and complexities additional to those considered in the valuation of traditional assets.

Web3

Web1 provided users direct access to websites offering previously unimagined amounts of data, access to knowledge, and connectivity. Web2 shifted the customer experience of the internet, combining new mobile technologies with information networks to allow the upload of user-generated content and leveraging the power of big data and nascent AI technologies to personalize and tailor the delivery of content via specialized apps. Web3 is the next iteration of the world wide web—a decentralized, blockchain-based online ecosystem. Platforms and apps built on Web3 aren't owned or governed by a central authority; rather, they are owned by network participants, who earn their ownership stake by helping to develop and maintain those services.

Zero-knowledge (zk) rollups

A zero-knowledge rollup is a layer 2 blockchain solution that performs computations and storage off-chain while funds are held in a smart contract. They take a different approach than optimistic rollups, using "validity proofs" to compute transactions off-chain, looking at only key data fields. This results in much faster processing times as hundreds of transactions can be compressed before being posted to the mainnet. The term "zero-knowledge" refers to the use of zero-knowledge proofs for on-chain transaction verification without requiring interaction or trust; they are cryptographic proofs that can demonstrate a statement's truth without disclosing any information about the statement itself.

IMPORTANT LEGAL INFORMATION

This material is intended to be of general interest only and should not be construed as individual investment advice or a recommendation or solicitation to buy, sell or hold any security or to adopt any investment strategy. It does not constitute legal or tax advice. This material may not be reproduced, distributed or published without prior written permission from Franklin Templeton.

The views expressed are those of the investment manager and the comments, opinions and analyses are rendered as of the publication date and may change without notice. The underlying assumptions and these views are subject to change based on market and other conditions and may differ from other portfolio managers or of the firm as a whole. The information provided in this material is not intended as a complete analysis of every material fact regarding any country, region or market. There is no assurance that any prediction, projection or forecast on the economy, stock market, bond market or the economic trends of the markets will be realized. The value of investments and the income from them can go down as well as up and you may not get back the full amount that you invested. Past performance is not necessarily indicative nor a guarantee of future performance. All investments involve risks, including possible loss of principal.

Any research and analysis contained in this material has been procured by Franklin Templeton for its own purposes and may be acted upon in that connection and, as such, is provided to you incidentally. Data from third party sources may have been used in the preparation of this material and Franklin Templeton ("FT") has not independently verified, validated or audited such data. Although information has been obtained from sources that Franklin Templeton believes to be reliable, no guarantee can be given as to its accuracy and such information may be incomplete or condensed and may be subject to change at any time without notice. The mention of any individual securities should neither constitute nor be construed as a recommendation to purchase, hold or sell any securities, and the information provided regarding such individual securities (if any) is not a sufficient basis upon which to make an investment decision. FT accepts no liability whatsoever for any loss arising from use of this information and reliance upon the comments, opinions and analyses in the material is at the sole discretion of the user.

Products, services and information may not be available in all jurisdictions and are offered outside the U.S. by other FT affiliates and/or their distributors as local laws and regulation permits. Please consult your own financial professional or Franklin Templeton institutional contact for further information on availability of products and services in your jurisdiction.

Issued in the U.S. by Franklin Distributors, LLC, One Franklin Parkway, San Mateo, California 94403-1906, (800) DIAL BEN/342-5236, franklintempleton.com–Franklin Distributors, LLC, member FINRA/SIPC, is the principal distributor of Franklin Templeton U.S. registered products, which are not FDIC insured; may lose value; and are not bank guaranteed and are available only in jurisdictions where an offer or solicitation of such products is permitted under applicable laws and regulation.

Canada: Issued by Franklin Templeton Investments Corp., 200 King Street West, Suite 1500 Toronto, ON, M5H3T4, Fax: (416) 364-1163, (800) 387-0830, www.franklintempleton.ca.

Offshore Americas: In the U.S., this publication is made available only to financial intermediaries by Franklin Distributors, LLC, member FINRA/SIPC, 100 Fountain Parkway, St. Petersburg, Florida 33716. Tel: (800) 239-3894 (USA Toll-Free), (877) 389-0076 (Canada Toll-Free), and Fax: (727) 299-8736. Investments are not FDIC insured; may lose value; and are not bank guaranteed. Distribution outside the U.S. may be made by Franklin Templeton International Services, S.à r.l. (FTIS) or other sub-distributors, intermediaries, dealers or professional investors that have been engaged by FTIS to distribute shares of Franklin Templeton funds in certain jurisdictions. This is not an offer to sell or a solicitation of an offer to purchase securities in any jurisdiction where it would be illegal to do so.

Issued in Europe by: Franklin Templeton International Services S.à r.l.–Supervised by the *Commission de Surveillance du Secteur Financier*–8A, rue Albert Borschette, L-1246 Luxembourg. Tel: +352-46 66 67-1 Fax: +352-46 66 76. **Poland:** Issued by Templeton Asset Management (Poland) TFI S.A.; Rondo ONZ 1; 00-124 Warsaw. **South Africa:** Issued by Franklin Templeton Investments SA (PTY) Ltd, which is an authorized Financial Services Provider. Tel: +27 (21) 831 7400 Fax: +27 (21) 831 7422. **Switzerland:** Issued by Franklin Templeton Switzerland Ltd, Stockerstrasse 38, CH-8002 Zurich. **United Arab Emirates:** Issued by Franklin Templeton Investments (ME) Limited, authorized and regulated by the Dubai Financial Services Authority. **Dubai office:** Franklin Templeton, The Gate, East Wing, Level 2, Dubai International Financial Centre, P.O. Box 506613, Dubai, U.A.E. Tel: +9714-4284100 Fax: +9714-4284140. **UK:** Issued by Franklin Templeton Investment Management Limited (FTIML), registered office: Cannon Place, 78 Cannon Street, London EC4N 6HL. Tel: +44 (0)20 7073 8500. Authorized and regulated in the United Kingdom by the Financial Conduct Authority.

Australia: Issued by Franklin Templeton Australia Limited (ABN 76 004 835 849) (Australian Financial Services License Holder No. 240827), Level 47, 120 Collins Street, Melbourne, Victoria 3000. **Hong Kong:** Issued by Franklin Templeton Investments (Asia) Limited, 17/F, Chater House, 8 Connaught Road Central, Hong Kong. **Japan:** Issued by Franklin Templeton Japan Co., Ltd., Shin-Marunouchi Building, 1-5-1 Marunouchi Chiyoda-ku, Tokyo 100-6536, registered in Japan as a Financial Instruments Business Operator [Registered No. The Director of Kanto Local Finance Bureau (Financial Instruments Business Operator), No. 417]. **Korea:** Issued by Franklin Templeton Investment Advisors Korea Co., Ltd. 3rd fl., CCMM Building, 101 Yeouigongwon-ro, Yeongdeungpo-gu, Seoul Korea 07241. **Malaysia:** Issued by Franklin Templeton Asset Management (Malaysia) Sdn. Bhd. & Franklin Templeton GSC Asset Management Sdn. Bhd. This document has not been reviewed by Securities Commission Malaysia. **Singapore:** Issued by Templeton Asset Management Ltd. Registration No. (UEN) 199205211E, 7 Temasek Boulevard, #38-03 Suntec Tower One, 038987, Singapore.

Please visit www.franklinresources.com to be directed to your local Franklin Templeton website.

The views and opinions expressed are not necessarily those of the broker/dealer; or any affiliates. Nothing discussed or suggested should be construed as permission to supersede or circumvent any broker/dealer policies, procedures, rules, and guidelines.

FRANKLIN TEMPLETON