Token due diligence: a structured approach to evaluate digital asset risk

February 2024

Building a better working world

Table of contents

Introduction

With more than 10,000 digital asset tokens tracked by CoinGecko in circulation, it may be difficult to ascertain quality from noise, memetic from consequential and groupthink from adoption. Though it may be likely that many of these tokens currently provide no tangible value to holders aside from a form of speculation and community engagement, a small subset may revolutionize the world as innovative disintermediation tools with robust value capture. The purpose of this framework is to provide a methodology when assessing exposure to tokens.

1. General token due diligence framework: a primer

A general risk framework to evaluate tokens can be organized in a multitude of ways. Some crypto-native firms have produced publicly available frameworks; some regulatory bodies, such as the New York State Department of Financial Services, are known to require coin-listing policies to meet rigorous standards; and other market participants presumably have privately held approaches for assessing tokens. Each of these players has its own risk tolerance thresholds, driven by internal risk management appetite, specific to an industry, or sector, and business model. As such, we have developed a token risk assessment framework that attempts to remain party agnostic and should be of interest to any entity interested in further assessing token risks.

For this paper, we define the following six risk pillars as a general representation of our methodology: reputational and strategic, technical, financial, legal and compliance, cybersecurity, and auditability. We will dive into several sub-risk categories for each pillar, as noted in the table below in bold.

We apply both technical and nontechnical lenses to this framework primarily to remain party agnostic but also because decentralized finance (DeFi), in its current state, is both technologically sophisticated and regulatorily immature. Therefore, risk disclosures prevalent in regulated consumer financial products generally are absent in cryptocurrencies. A sufficient mix of technological due diligence and research on external project factors must be conducted for proper baseline coverage.

This framework is not all-encompassing, nor will we touch on all sub-risk categories in this paper, but it should provide the reader with a preliminary framework that can be further built upon as the industry continues to evolve.

Reputational and strategic	Technical	Financial	Legal and compliance	Cybersecurity	Auditability
▸ **People and entity** ▸ Environmental, social and governance (ESG)	▸ **Network design** ▸ **Smart contract risk** ▸ **Upgrades and maintenance**	▸ **Tokenomics** ▸ **Financial metrics and ratio analyses** ▸ Treasury management	▸ **Securities analysis** ▸ Compliance ▸ Illicit or criminal activity	▸ Governance and operational security	▸ **Audit and ownership**

2. Reputational and strategic

2.1 People and entity risk

While it may be common to suggest that autonomous code will control the future of on-chain transactions, the participants behind the code at the social layer often have an immense impact and are commonly overlooked. A foundational consideration for a token is whether the core team members have elected to operate as anonymous or as public figures. Often, linking one's real-life identity to on-chain activity can bring credibility and legitimacy to a project. However, teams often decide to build anonymously for a variety of reasons, including regulatory risk, personal privacy and reputational risk.

Teams that build with non-anonymous founders have demonstrated high levels of accountability and success. Ethereum, Solana, Uniswap, Maker, Aave and Compound are examples of projects with public founders that have sustained billions of dollars in total value deposited into the protocols they have built. These projects have built great user experiences and generated revenue over the last two years.[1] Even during bouts of high market volatility and an extended "crypto winter," these projects have demonstrated talent retention, community engagement and continuity in building new products. When considering initial or even follow-on funding rounds to finance operations, establishing relationships with accountable, public leadership may help assuage investor concerns and allow for greater interoperations between portfolio companies and that entity. On the other hand, however, some public founders are known to have experienced major faults in execution. These founders typically did not launch decentralized networks or projects, but rather used a token launch to market their centralized lending platform or exchange. Using their public credibility may have allowed these entities to increase leverage or misappropriate funds using their centralized company and token as an opaque layer sitting above the underlying problems.

Comparatively, anonymous founders have demonstrated more mixed track records. Satoshi Nakamoto has been the most successful anonymous founder to date in terms of token market cap, but Satoshi may be the exception rather than the rule. There have been a slew of application layer protocols, with anonymous founders or core team members, that have not ended well for investors. Potential fraudulent behavior aside, by nature of their anonymity, protocols with anonymous founders can be very difficult to hold accountable. Although there appears to be a relationship between success of a project and non-anonymous founders, this does not implicitly suggest a deterministic link. It is therefore imperative to use judgment when incorporating this evaluation into a due diligence review. It is likely more appropriate to use this criterion as a means of gaining comfort that there is a single individual (or group of individuals) who can be assigned accountability. They have chosen to put their skin in the game by staking their reputations on the success of the protocol and assume the risk of any nefarious activity.

3. Technical

3.1 Network design

The design of the underlying Layer-1 (L1) blockchain network is the basis in which any application-level token must operate and dictates the conditions in which the native cryptocurrency blockchain settles transactions. Therefore, several decisions are made based on the use case of the network itself. These decisions often represent an attempt to solve the blockchain trilemma of optimizing a network's scalability, decentralization and security. Generally, projects choose to focus on two out of three based on the goal of the network itself. For example, a project intended to have higher throughput and lower transaction fees on its network may choose to optimize for scalability and security at the expense of decentralization by relying on a small set of validators nodes that run expensive or specialized hardware.

What degree of decentralization is enough for censorship resistance? This is a difficult question to answer, as it cuts at the purpose of public blockchains in general: a censorship-resistant, credibly neutral, decentralized platform open to all. Without these properties, the value proposition of public blockchains is far less compelling, and what remains is a centralized and computationally inefficient database. Therefore, maintaining a high level of decentralization is mandatory to protect against the risk of censorship at the network level.

Balaji Srinivasan attempted to measure decentralization by proposing the Nakamoto Coefficient, a quantitative measure of a system's decentralization, motivated by the well-known Gini Coefficient and Lorenz Curve.[2] The Nakamoto Coefficient represents the number of validators

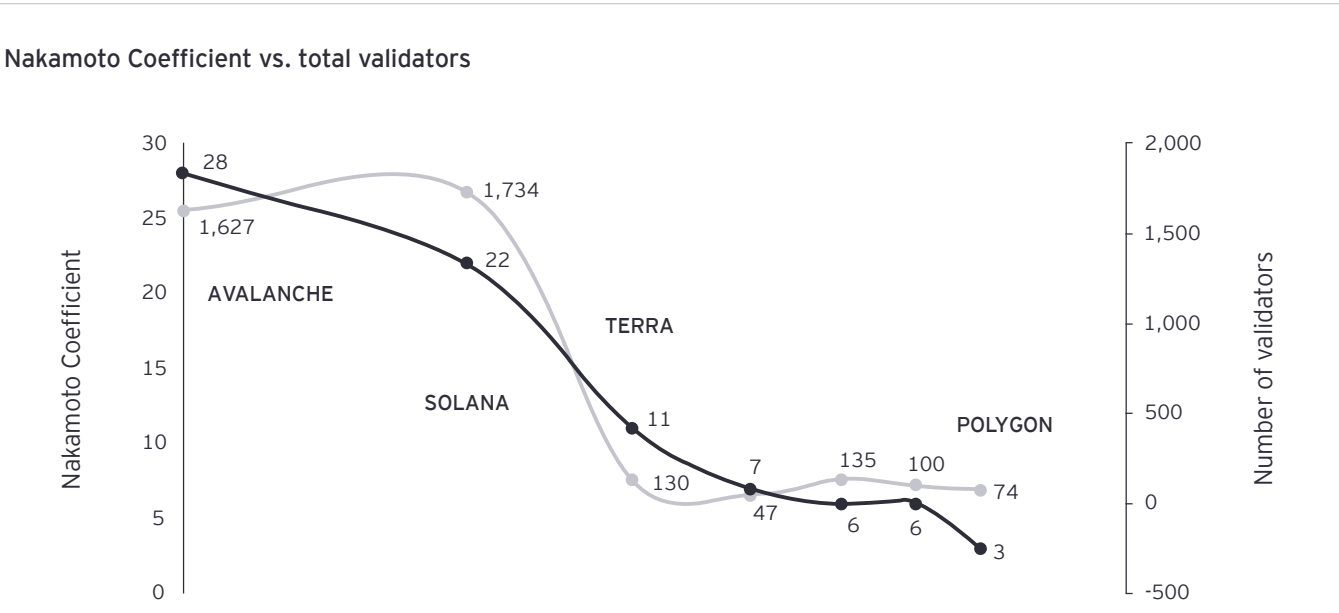

Figure 1 : Nakamoto Coefficient among L1 protocols as of 2022.

(nodes) that would have to collude together with malicious intent to impact the safety or liveness of the blockchain via invalid state transitions, distributed denial of service (DDOS) or block reorgs.[3]

On the surface, this may seem like a trivial exercise if you know the method of consensus and a few other public data points; however, Srinivasan expands on this calculation by considering several components of centralization that are measured at what he calls the "subsystem" level. These subsystems represent components of a public blockchain ecosystem that can potentially compromise decentralization of a public Layer 1 network. If one of these subsystems is found to be centralized, then an argument can be made that the entire system is centralized. Therefore, determining which subsystems are critical to a Layer 1 network must be a key consideration when attempting to calculate the Nakamoto Coefficient using this methodology.

Subsystem	Centralization metric	Definition
Mining subsystem	Block reward	Measures distribution of the block reward over 24 hours
Client subsystem	Codebase	Measures the distribution of client implementations (e.g., GETH vs. Parity)
Developers subsystem	Commit	Measures the number of engineers who have made commits
Exchange subsystem	Volume	Measures the volume traded across multiple exchanges
Node subsystem	Count	Measures node distribution across countries
Ownership subsystem	Address	Measures the number of unique addresses that contain an amount of the asset between a predetermined threshold

Figure 2: Subsystems of blockchains

3.1.1 Decentralization

The higher the Nakamoto Coefficient relative to the total number of validators, the lower the risk of collusion disrupting a decentralized blockchain. Avalanche and Solana demonstrate higher levels of decentralization based on the Nakamoto Coefficient than the more centralized chains in the lower right quadrant, such as Polygon or BNB Chain. Centralization can lead to a higher risk of collusion at the validator level, allowing invalid blocks to be published or censorship in the case scenario. In proof of stake chains, networks also run the risk of less than two-thirds of validators (either total validator nodes or combined stake weight) online at any given time, which can lead to forks and deep block reorgs as nodes struggle to reach consensus and finality. Centralization can compromise credible neutrality as in the case of BNB Chain, where a proof of authority version of Tendermint's consensus framework allows for only 21 active validators. In October 2022, a malicious actor was able to steal $100 million in BNB, the chain's native cryptocurrency. The attack was ultimately hindered due to the validators' ability to coordinate, identify the attack and halt the network, restricting the hacker's ability to move the assets elsewhere. Although a case can be made that the viability of the network was saved due to its centralization, its credible neutrality is unclear, which could introduce risk to token holders.

3.1.2 Bridging

In addition, there are other technical design risks, aside from collusion at the consensus level, that blockchain protocols must contend with. Much of the L1 ecosystem today is built on cross-chain activity. Many users rely on bridges from Ethereum to move assets back and forth by passing inter-blockchain messages. As bridges are inherently less secure due to reliance on more centralized security models, there are obvious trade-offs to make when bridging assets cross-chain. For example, holding non-native tokens from one blockchain on another blockchain (such as wrapped bitcoin) incurs several risks of exploit, assuming these ecosystems do not share a common settlement layer.[4]

As an example, the Wormhole Bridge was exploited for 120,000 ETH. When ETH tokens are bridged from Ethereum to Solana via Wormhole, they are locked in a contract on Ethereum and subsequently minted on Solana. The attacker bypassed the verification process of the Wormhole Bridge on Solana and successfully generated a malicious message that specified 120,000 Wormhole ETH (wETH) to be minted.[5] The attacker then transferred 93,750 wETH back to Ethereum, which resulted in the same amount of wETH on Solana unbacked. This event introduced a level of systemic cross-chain risk that required a significant capital injection from Wormhole's parent company as a backstop.[6]

3.1.3 Architecture

Additional risk considerations related to network design can also include a review of the blockchain's architecture. For example, the concept of modular vs. monolithic blockchains can have a significant impact on scalability and security. The concept of modularity is important because it allows blockchain networks to outsource certain activities that are performed traditionally in monolithic blockchains, including consensus, data availability, execution and settlement. Ethereum's commitment to modular architecture principles is seen in its proto-danksharding roadmap. Ethereum's progressively modular design will allow it to enhance its ecosystem's economic security by ensuring settlement will always happen at the Ethereum base layer. Overall, a robust architecture will increase security and provide more flexibility in design.

3.1.4 Governance

Governance is also a risk to holders of both tokens issued through smart contracts or base cryptocurrencies (ETH / Bitcoin). Governance is generally designed into the operation of the network or decentralized application through the implementation of an economic coordination layer. Through governance processes, token holders are able to coordinate efforts to change, update and protect the network. In 2022, Juno protocol, part of the Cosmos (ATOM) network, identified a prospective Sybil attack and began pre-emptively preparing for it as the token generation event (TGE) neared.[7] The Juno attacker created 50 wallets with 50,000 ATOM tokens, each entitling the attacker to 2.5m Juno tokens initially and more than 3m after staking rewards. The attacker's actions broke the intent of the airdrop rules that stipulated a maximum of 50,000 Juno tokens per 50,000 ATOM tokens. The Juno community took time to deal with the issue, which led to a contentious governance vote that split the community between those who felt the Juno tokens should be

confiscated from the attacker's account vs. those who believed the mistake should not be remedied.

In a precedent-setting vote, the community passed Proposal 16, which confiscated a single individual's wealth by performing a hard fork to rewrite the state of the network's ledger. Although the action was taken for seemingly altruistic purposes, many consider this a blight on credible neutrality of public blockchains. On one hand, the attacker in this case did not take advantage of a technical exploit; rather, they took advantage of a social exploit based on publicly available information. On the other hand, this event represented a near-existential risk for the protocol and the vote was put up to the community. In either case, all players were aware of the risks involved and potential outcomes, and the community voted to protect itself. When considering governance, it is vital to research the following: Who has the most say (often, the most tokens)? Does a vote actually result in action being taken by the team? What controls are in place to combat governance attacks?

3.2 Smart contract risk

A smart contract is a self-executing digital agreement that enables two or more parties to exchange anything of value in a transparent way without the need for custodial intermediation.[8] Smart contracts have become a powerful way to build DeFi-integrated products through disintermediation and composability, allowing contracts to interact with one another. Ethereum is the most widely used (by total value locked (TVL)) general-purpose smart contract blockchain with 63.1% of TVL in DeFi applications out of all L1 blockchains as of October 2023.[9]

The majority of Ethereum contracts are written in Solidity or Vyper, with Solidity commanding the lion's share of development activity.[10] Solidity was designed to be simple and easy to use with many influences from C++, Python and JavaScript.[11] There are robust, public smart contract libraries, testing frameworks, tooling and community support because of the Ethereum Virtual Machine (EVM) network effect. Solidity has known vulnerabilities as well and should not be considered "risk free" based on its dominance alone.[12] In fact, hacks, bugs and other exploits are an ongoing issue despite the ubiquity and transparency of smart contracts written in Solidity. Using tools to review smart contracts can be an efficient way to leverage the wisdom of the crowd and capitalize on the network effects mentioned above. The EY Smart Contract Review Tool (SCRT) has already been used successfully in this manner because the SCRT not only is designed to run tests against a library of commonly known exploits but also offers customizable functionality that allows testing against "what-if" scenarios. Figure 3 displays several examples of exploits on EVM (including non-Ethereum) chains.

One common type of exploit is a flash loan exploit. A flash loan allows any participant to borrow a significant amount of undercollateralized capital if it is returned within the same transaction block that the loan originated in. Flash loans showcase the power of DeFi composability. They democratize access to arbitrage opportunities and facilitate folded leverage transactions and seamless collateral swapping. Since flash loans must be repaid within the same transaction, the cost of borrowing is only the cost of computation (gas). If the loan is not repaid, the entire transaction reverts.[13]

Protocol	Dollars (in millions)	Date	Exploit	Chain
Harmony	$100.0	6/24/2022	OpSec	Harmony
GYM	$2.1	6/10/2022	Smart contract exploit	BNB
DEUS DAO	$13.7	4/28/2022	Blockchain oracles	Ethereum
Beanstalk	$182.0	4/18/2022	Flash loan	Ethereum
Inverse Finance	$16.0	4/2/2022	Oracle	Ethereum
Ronin	$625.0	3/29/2022	Sybil	Ronin

Figure 3: EVM chain hacks

Flash loans are not inherently nefarious; however, they can be used to facilitate technically complex manipulations through traditional blockchain infrastructure that can be motivated by malicious intent. As an example, a flash loan exploit occurred when a malicious entity, via smart contract, borrowed a significant sum of capital from a lending protocol that was then used to manipulate market pricing, causing an artificial arbitrage opportunity. This, in turn, allowed the user to accumulate a large amount of a single token and conduct a Sybil attack on protocol governance, which allowed it to push a nefarious proposal through formal governance channels. This resulted in the entity's ability to drain the token's primary liquidity pool and then repay the loan all in the same transaction, netting $186 million in profits.[14]

Other smart contract risks include unaudited codebases. Companies, such as Trail of Bits, provide smart contract auditing services that review contract code for flaws and return a report that can be posted on the protocol's website to demonstrate transparency. However, not all protocols use auditing services, and not all auditing services are the same. Additionally, the availability of a report does not necessarily indicate a "seal of approval" or represent a form of assurance in the same way an audit opinion does. In most cases, reports will identify code flaws and provide remediation activities, but there is no simple mechanism to ensure that all items have been addressed by the project team short of monitoring future code commits through a code repository.

Even with audited codebases, it is important to consider vulnerabilities in popular code libraries, especially from newer chains. In 2022, a vector vulnerability in the Solana Program Library, a repository of many code implementations for specific programs and functions, could have allowed exploiters to drain the entire TVL of several protocols. The vulnerability was present due to a rounding error through which users could have continuously deposited and withdrawn funds until several DeFi protocols were drained, thus making a profit from the rounding error, minus Solana network fees which are, by design, very low. Notably, this attack would not have been feasible on Ethereum due to higher transaction fees as a means of Sybil resistance.

3.3 Maintenance and upgrades

Despite what a token is designed to do, there will always be the question: Who will maintain and upgrade the codebase?

At the blockchain level, independent organizations, such as the Ethereum Foundation, fund active research and development of the core protocol specifications to be implemented by execution and consensus layer client teams. The research team is composed of experts in computer science and cryptography. As an example, EIP–1559 introduced a transaction-pricing mechanism called the base fee. As a function of past block demand, the base fee adjusts gradually to help smooth expected transaction fees on Ethereum and is subsequently burned from total supply. Concurrent to the base fee adjusting, Ethereum block sizes adjust to allow greater throughput during periods of high block demand, resulting in the base fee increasing to dissuade marginal transactors via higher costs to promote an equilibrium. EIP–1559 took about two years to implement from its initial code repository creation due to the robustness of the EIP implementation process.[15]

The key components regarding protocol maintenance are twofold. First, the level of transparency in governance processes is vital. More transparency provides the public more opportunity to weigh in on, scrutinize and advocate for changes that the community aligns with. In more mature environments, such as Ethereum, the risk of malicious code making its way into production is significantly less due to the amount of visibility inherent to the EIP governance processes and amount of Ethereum community engagement in vetting proposal concepts and source code. The same cannot be said for most newer protocols that do not have the commensurate levels of engagement. Therefore, it is imperative to scrutinize token governance processes to understand the level of activity, the major players and personalities, and the concentration of voting power. And second, transparency of source code provides an easy way to determine whether a protocol is using public, battle-tested code libraries.

3.3.1 Layer-1 protocols

Many L1 protocols are not yet sufficiently decentralized, and project teams often have direct control over software upgrades and business development. Typically, these protocols have a form of limited on-chain governance abilities. This can be considered higher-risk protocol management because it allows for unilateral decision-making. By maintaining a centralized development team, the broader community is unable to develop organically, and community input may be overlooked. Organic community development has a strong correlation to economic sustainability due to the formation of a social consensus around values-based Schelling points instead of monetary considerations. Inorganic communities collapse as they coordinate around the speculative returns of the native token, the Terra Luna saga being the prime example. It is, however, unlikely that many projects start from a fully decentralized model. A measure of centralization is often required to initially bootstrap activity and coordinate efficient decision-making, which is critical in early-stage protocol development. The important factor to take into consideration here is whether the project team has publicly released a project roadmap with a clear path to decentralization, and if the team has followed its roadmap.

3.3.2 Decentralized applications

At the application layer, in most cases, development activities are managed by a combination of community decentralized autonomous organizations (DAOs) and core developer teams. DAOs typically set community funds aside for this purpose from the token generation event to compensate their developers. In addition, DAOs often fund further protocol development and community engagement through grant programs or liquidity incentives.[16] On-chain DAO governance proposals can be used to implement protocol changes as needed. DAOs give token holders varying degrees of governance rights to vote on and implement changes executed by a governance smart contract.

To subsidize community involvement similar to a project manager or product developer, DAOs may offer monetary incentives in a consulting-like capacity for those in the community engaging with the protocol developers. Outsourcing certain roles to the community, especially when the community owns the governance tokens, can be an important way for DAOs to develop new products that fit the community's needs. Therefore, for both paying its employees and the community, a sizable cash runway is near mandatory for protocol longevity until it may be self-sustaining based on positive cash flow.

Bull markets tend to coincide with significant speculation on governance token prices, which are another medium for DAOs to incentivize participation from the community. Though impossible to foretell, token price can serve as a barometer for the marginal new user or speculator in a reflexive manner. Token incentives for the more speculative may be an attractor for greater development and community engagement, but not to such a degree that token supply is concentrated in a small number of insiders' wallets.

While governance may appear to be decentralized and effective for certain decentralized applications and communities, patterns of behavior would suggest that governance is as robust as the core team's credibility and track record. Naturally, when a community believes it passed a vote, one must consider whether the core members, who often hold the authority to enforce that vote, will follow through with the action.

4. Financial

Financial analysis is a core component when considering the viability of a token. As with any currency, in-game item or revenue-generating entity, a protocol's token must provide a reasonable inflation or deflation rate, utility in some way, and some sort of value capture.

Tokenomics are the economics of the token, and the concept generally encompasses token supply, emissions schedule, distribution, lockups, vesting, staking rewards and other incentives, including burning, vote locking and more.[17] As tokenomics are based on a combination of the preceding factors, they naturally can come in many combinations that can significantly impact the token's price over the medium to long term.

In addition to tokenomics, a token can be evaluated based on a few key metrics, such as market cap, fully diluted value (FDV), circulating supply, revenue per token and TVL. Using these metrics to perform ratio analyses, such as FDV to TVL, can create a benchmark KPI to cut through the token supply and evaluate a protocol on the

economic activity and utility supporting its valuation. When considering TVL, however, it is important to consider whether there is a corresponding burn, buyback or profit distribution from the TVL. Uniswap, for example, has a high TVL, but all "revenues" flow back to liquidity providers rather than anyone holding the UNI token.

4.1 Tokenomics

4.1.1 Layer-1 protocols

L1 blockchains have varying degrees of tokenomic design mechanisms. For example, a proof of work chain, such as bitcoin (BTC), rewards miners 6.25 BTC plus fees per block mined as of October 2022.[18] Miners compete to solve the nonce per varying algorithmic difficulties, and the winner has the right to propose the next block on the longest chain. Bitcoin has a hard cap of 21 million coins and reduces block rewards about every four years until the hard cap is reached in 2140. Other L1 chains, such as Ethereum proof of stake, reward validators for participating in consensus by attesting to the validity of a block (enforcing the fork choice rule) and proposing blocks.[19] While Ethereum does not have a hard cap in total token supply, the transition to proof of stake combined with EIP–1559 has resulted in ETH becoming a deflationary asset as more ETH is burned per transaction than issued.[20] From the perspective of risk and protocol viability, a token holder should not exclusively interpret whether an asset is net inflationary or deflationary as positive or negative; rather, the token holder should assess the mechanisms that are used to achieve either status, such as token burns from revenue or the impact of inflation on trading order books. For example, if ETH reduced its inflation rate by 90%, from about 4% to about 0.4%, all else equal, there is 90%, less daily sell pressure due to inflation reduction. Further, the transition from proof of work to proof of stake reduced mandatory sell pressure, as fiat-based mining costs covered via ETH sales are no longer required.

L1 protocols can also use experimental economic design mechanisms as part of their tokenomics. Terra was unique in that an algorithmic stablecoin was embedded into the protocol design. The native cryptocurrency, Luna, was designed to algorithmically back the stablecoin US Terra (UST). To mint UST, an equal amount of Luna would be burned.[21] One UST could always be minted for $1 worth of Luna, making arbitrageurs profitable as this incentivized peg maintenance of UST to $1. This protocol design proved to be catastrophic. Terra collapsed under a reflexive negative spiral as UST holders lost faith and sold UST either for other stablecoins or minted Luna to later sell, causing other more-leveraged Luna traders to sell via forced liquidations. In essence, the market cap of Luna (along with an accrued treasury or retained earnings) should have always been greater than the value of UST to backstop the peg, which is difficult for a free-floating and highly volatile cryptocurrency. In the aftermath, it was clear that the asset/liability mismatch was not well understood by most participants in the crypto community.

4.1.2 Decentralized autonomous organizations (DAOs)

DAOs provide a vastly different value profile than an L1 blockchain. Whereas L1 blockchains give users a storage and computation engine, DAOs can deliver any form of value to their users, including gaming, DeFi, art and more. L1 blockchains often have a more visible and endogenous revenue capture model as well, allowing fees that users pay to the network to flow to the computers that execute transactions and agree on the latest state. DAO tokens, on the other hand, may appear more related to community memberships or decentralized business entities and need to exhibit utility and revenue capture. When it comes to utility, the choices are manifold. As examples, some DAOs may require the token to enter its game, to own the token to provide first-loss capital in lending or insurance to earn fees or more token supply, or to simply vote on where DAO treasury money may be spent to grow the community. In many circumstances, there may be value for an individual to own the token, but tangible value on a market level may not be present.

As such, in 2022, most governance tokens were down more than 90% and continue to have major dilutive issuance with low floating supply and high FDVs. Figure 4 exemplifies Solana ecosystem tokens that are widely reported to have low-circulating supply and high inflation. And further, it can be difficult for DAOs to gain tangible value due to prevailing securities laws, where venture capital may be less likely to fund a DAO that distributes earnings to its token holders due to difficulty in providing clarity that the token is not a security. To work around cash flow distribution, some communities have voted on "token buybacks and burns" to buy existing supply and then burn it in an attempt to boost price. When researching DAOs, users should understand how total supply will change over time and how the DAO generates revenues to fund operations and token purchases. While there are a variety of different supply models, such as vote-escrowed and protocol-owned liquidity, it is possible those mechanisms provide more volatility due to lower-circulating supply rather than tangible underlying value, despite arguments suggesting that higher vote weight (and thus inflation weight) is beneficial for all token holders.

Asset	Price	Market cap (in millions)	FDV (in millions)	Market cap/FDV	TVL (in millions)	FDV/TVL	ATH	% of ATH	Cash flow to holders Y/N
SOL	$13.41	$4,882 (no max supply)	$4,882 (no max supply)	100%	$312	15.6	$259.6	-94.8%	Y
MNGO	$0.01	$26	$71	23%	HACKED	HACKED	$0.5	-97.2%	N
SRM	$0.27	$100	$2,761	4%	$1	2,761.0	$13.8	-98.0%	Y
RAY	$0.19	$29	$105	28%	$50	2.1	$16.8	-98.9%	Y
TULIP	$1.30	$2	$12	16%	$23	0.5	$50.2	-97.4%	N
SLND	$0.41	$12	$42	29%	$30	1.4	$16.7	-97.5%	N
SBR	$0.001	$2	$13	12%	$25	0.5	$1.0	-99.9%	N

Figure 4: Solana ecosystem tokens
Sources: CoinGecko, DefiLlama. Data as of 17 November 2022.

4.2 Financial metrics and ratio analyses

4.2.1 Layer-1 protocols

L1 protocols may have a more universal model, at least for monolithic chains, than other tokens. For L1s, revenue is produced when users transact on the platform and pay fees. Fees may be in computation, storage, verifying proofs, verifying data availability or any combination. For modular chains, the greater the usage volume, the greater the revenue, all other things being equal. Where fees flow is arguably even more important, which dictates who receives fees and inflation on the protocol. Some L1s may distribute all fees to stakers, whereas some may take a percentage for their own treasury in a more for-profit manner. The relation between fees and inflation is also a strong indicator of user adoption, usage and demand for blockspace. For example, a protocol with 100% inflation and 1% fees (as a percentage of market cap) has a far different market dynamic than a protocol with 0% inflation and 4% fees, all else equal. When considering financial metrics and ratios, protocol revenue (R), market cap to revenue (MC/R), stock to flow (S2F) and staking yield are helpful metrics. Because stakers tend to receive all fees and inflation, any non-staker will be debased due to inflation and will have an opportunity cost in fees and inflation forgone. Therefore, the marginal staker will receive their share of the total market cap multiplied by inflation and fees as a percentage of market cap.

Example: User X holds Token Y at $1b market cap and holds 50% of all stake, 10% is staked, and there is 5% inflation + fees. User X holds $1b * 10% * 50% = $50m of Token Y. User X's $50m stake is entitled to $1b * 5% inflation + fees * 50% stake = $25m, or a 50% annual return from inflation and fees.

Other financial metrics may include TVL to market cap, total transactions and transaction volume. However, there is not a direct link between any of those and yield for stakers across protocols. One protocol may have low transactions but high fee value; some high transaction-volume protocols may have negligible fees and may not even flow in full to stakers. Hence, each L1 protocol should warrant its own analysis, but consideration should be given on how to accrue protocol revenue and the breakdown between fees and inflation.

4.2.2 Decentralized Autonomous Organizations (DAOs)

DAOs may generate revenue when users interact with their smart contracts, in-game items and more. It is entirely DAO dependent, but each respective subsector (DeFi, gaming, art) tends to have its own drivers. For DeFi, TVL tends to be a strong correlative metric, but only if the TVL has a percentage of either TVL or yield that flows back to the token holder or token-guided treasury. For gaming, it could be a blend of active users, revenue from in-game activities, whether the DAO made a blockchain, whether a DAO has a treasury earning yield, and whether there are in-game advertisements. Art can be similar but relies more on primary issuance of new non-fungible tokens (NFTs) and royalty fees from secondary market volume. There may be partnerships with metaverses or games as well. In addition, total supply, especially floating supply to total, is key for assessing the dilutive path of token issuance over time. For DAOs, how revenue is generated; where it flows; and the underlying sustainability of its userbase, fees and supply are of utmost importance.

5. Legal and compliance

5.1 Securities analysis

Is it a security? This is a question that has been repeated ad nauseum since cryptocurrencies hit the mainstream and one that has yet to be sufficiently resolved. In 2018, then U.S. Securities and Exchange Commission (SEC) Chairman Jay Clayton provided some clarity to this question by drawing a distinction between cryptocurrencies that seek to replace sovereign currencies and those that represent an investment in a common enterprise: [22] the former not being considered a security and the latter being considered a security. This characterization drew a direct connection to the Howey Test, which is the pre-eminent framework for assessing whether an asset constitutes a security as defined in the US Securities Act of 1933. Even though much has changed since 2018, applying the Howey Test is still the main way to assess all different types of digital assets from a securities perspective. However, there is increasing pushback from major crypto players that the Howey Test, as it is currently defined, is not nuanced enough to account for factors such as decentralization with regard to definitions such as "common enterprise." In general, though, a broad application of the Howey Test can be considered as a tool for providing baseline considerations when attempting to determine whether a cryptocurrency should be classified as a security.

Forman, 421 U.S. at 853, states that "... holding that a security does not exist 'where [a consumer] purchases a commodity for personal consumption or living quarters for personal use.'"

These distinctions, while subtle, begin to draw a line around what type of tokens are more like securities than others. For example, tokens such as ETH (at this time, not considered a security by the SEC) that aim to act as a store of value, medium of exchange, unit of account, provider of economic security and metering token for computation on Ethereum have practical uses that may transcend speculation or expectation of profits for holders. However, Gary Gensler, current Chairperson of the SEC, has proven to be much more hawkish in his classification of digital assets, hinting in public statements this his goal will be to treat almost all digital assets, including cryptocurrencies, stablecoins and NFTs, like securities. Under his leadership,

the SEC has also primarily applied a regulate by enforcement strategy rather than rulemaking specific to digital assets. This approach appears to be based in part on prepared remarks he provided in April 2022, where he noted the SEC should remain technology neutral in its application of securities law. Gensler doubled down in May of 2023 [23] during his keynote speech at the Atlanta Financial Markets Conference where he is quoted as saying the "rules have been published" insinuating that his SEC's position on securities will not adapt to accommodate assets deployed on decentralized networks, but stands ready to support crypto natives' path to compliance under the existing regulatory framework. This approach has led to a myriad of court cases (the SEC has engaged over 100 enforcement actions today) that have led to conflicting guidance as to how digital assets fit under the Howey Test. Most notably, in July of 2023, courts ruled in favor of Ripple Labs by affirming that the company did not violate securities law by selling its XRP token on a public exchange. The judge acknowledged that those sales constituted blind bid/ask transactions — a notable win for the crypto industry, albeit one that came with a large and confusing caveat. In the same ruling, the courts also found that Ripple's $728.9 million sale of XRP to hedge funds and other sophisticated buyers did constitute a sale of unregistered securities, the nuance being that Ripple's marketing efforts to these buyers made it clear that the "company was pitching a speculative value proposition," one that was dependent on the efforts of the company to build and develop the blockchain infrastructure that supported the XRP token.[24] This ruling highlights an important point for both retail and institutional investors when assessing legal or regulatory compliance risk using the Howey Test; that you must pay attention to how cryptocurrencies are marketed. This is a prong of the Howey Test that is still very relevant and can be used to identify potential red flags. In this era of instant communications via social media and other communications apps, it is all too common that project teams will publicly advertise unrealistic returns predicated on future token functionality or systems of value accrual that requires further development. These messages are very often amplified and propagated by paid advertisers who do not disclose their monetary stake, insiders with large pre-sale token allocations, and community members all who are reliant on increasing liquidity to actualize the profits they have been promised. The result usually ending with non-insiders experiencing significant loss as exit liquidity for those who were most vocal about the potential for making profits. It is therefore important to pay attention to how the project team conducts itself in public forums such as social media and other community engagement platforms and the size and recipients of pre-sale token allocations whether directly through token issuance or indirectly through token allocations to marketing budgets. It is pragmatic to avoid tokens or projects that provide large token allocations to founders or consultants or explicitly market outsized returns or guarantees of a token's future value accrual without a clear business model and technological roadmap that supports the numbers. The old adage of "if it sounds too good to be true, it probably is" still rings true in cryptocurrency markets.

While regulators in the US still grapple with the regulatory question, their counterparts in the European Union have been working hard to implement a set of rules for the crypto industry. EU regulators established the digital asset specific regulation, Markets in Crypto-Assets (MiCA), with the intended purpose of creating a unified set of crypto rules that can be applied to various crypto assets and their related activities and services. The success of this regulation could provide a framework for other countries to use, which could lead to the export of these rules to other jurisdictions.

6. Cybersecurity

6.1 Governance and operational security

Understanding the governance processes and operational security hygiene of teams building on and supporting both L1 networks and the smart contracts deployed on top of them is a critical factor in understanding the risks associated with the tokens supported by them. If a bug is exploited or hack is successful, it is highly likely that any funds lost are completely unrecoverable due to the immutable nature of blockchain transactions. There is also no guarantee that an exploited code flaw can be successfully remediated in a timely manner. It is imperative that project teams have robust cyber risk management processes when developing smart contracts and managing the private keys and wallets that control protocol or community funds, as well as proper governance procedures to identify and address potential vulnerabilities. The complexity of these processes, and therefore risk, increases in tandem with the level of decentralization introduced into governance processes. Through ongoing distribution of governance tokens, project teams incrementally dilute their ability to exercise control over the direction of their protocol in favor of decentralized, community-driven governance processes. While this approach embodies the ethos of cryptocurrencies, it can also expose the pitfalls.

Take, for example, the Compound Finance smart contract exploit that occurred in October 2021. A malicious actor discovered a vulnerability in the Compound Comptroller contract, which is the risk management layer of the Compound protocol and controls the token market interest emissions. The result was that roughly $80 million in excess COMP (Compound's governance token) was incorrectly distributed.[25] Cybersecurity management frameworks would generally classify this as a vulnerability that would require immediate patching. However, immediate patching was impossible as Compound's governance processes were designed to operate based on a decentralized model. In April 2020, Compound Labs initiated its decentralization roadmap by deploying its Governor Bravo smart contract, enforcing programmatic governance. This included removing any single individual with administrative privileges and introducing a time lock feature coded into the smart contract itself enforcing automated, programmatic governance controls over processes like change management. The time lock feature enforced a two-day "cooling-off" period for the community to perform any last-minute diligence on the contract itself and the impact that approved changes to the protocol may have.

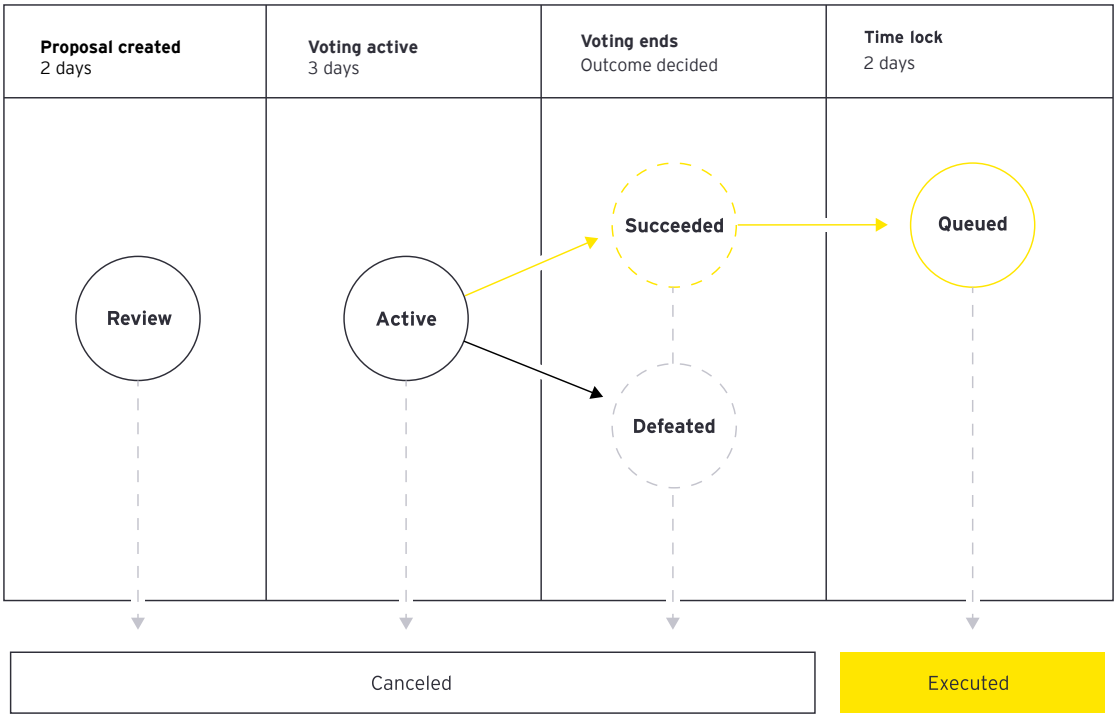

Figure 5: From Compound

It should be noted that the Compound protocol does include a Pause Guardian function that can be called in the event of an emergency exploit, where the authority to pause the protocol's operations is controlled by Compound Labs via a multi-sig wallet. However, Compound's Comptroller contract was not managed by this multi-sig wallet; thus, the Pause Guardian function could not be used to bypass community governance. Therefore, this exploit remained vulnerable for multiple days after it was identified due to the same processes that were meant to help mitigate these risks. Understanding how governance processes work and the extent a project team or other centralized entity has administrative control should be a key consideration for token holders as it impacts their ability to understand and monitor how protocols or project teams are actively managing risks attributed to cyber incidents. Reviewing and understanding a protocol's history of governance proposals can provide insight into the number of exploits, potential attacks and attack remedies. Poor or improperly designed risk management processes, particularly related to cybersecurity, can manifest in risk events that directly impact a protocol's long-term viability.

DAOs also present a significant vector for attack, particularly when a protocol implements a community-controlled treasury wallet or general fund. Multi-sig wallets are a common practice to help protect funds in these types of communal wallets, wallets by distributing signing authority to multiple individuals. However, project teams or responsible community members are not always completely transparent in terms of who has control of the signing keys and the level of rigor of their key management practices. It is therefore important to understand both how a multi-sig wallet is implemented, who controls those keys, and how the keys are stored; a multi-sig wallet is useless if the keys themselves are controlled by highly centralized actors or stored in an unsecure manner.

7. Auditability

7.1 Auditability and ownership

The degree to which a digital asset's existence or a transaction related to a digital asset can be verified using on-chain data should be taken into consideration when evaluating risk associated with a cryptocurrency or token. Transactional data is publicly available, but the average user relies on third-party block explorers or APIs to retrieve and visualize it, and it should be therefore treated as an external source of information that requires additional diligence in order to be used as a trusted data source. At a minimum, the completeness and accuracy of data should be tested and, if possible, sourced from multiple parties. However, if the rigors of a financial statement audit are applied to the analyses, then the relevance and reliability of information from a blockchain would be a key audit consideration and therefore require additional evaluation of the source and nature of the data. If blockchain data is unavailable and block explorer data is unreliable, this can lead to loss of funds; significant operational hurdles; and difficulties when reporting to regulators, auditors or other third parties and in effectively managing risk.

A token holder should be able to very clearly understand how ownership is defined within the blockchain network on which they are operating. For example, the Cosmos blockchain has a native "clawback" functionality that allows the issuer of an asset the ability to burn clawback-enabled assets using an administrative function that effectively destroys the asset and removes it from the owner's balance. This is a conscious design decision because it helps enable development of SEC-compliant assets; however, such a design decision also presents the risk of a clandestine and arbitrary confiscation of account funds by malicious entities. Additionally, the token holder should understand the rights that are afforded to them through token ownership and how those can change based on how the token is being used for various DeFi activities, such as staking or providing liquidity.

Additionally, the degree of transactional visibility is important for token holders to be able to audit existence, movement and ownership of digital assets. The data necessary to trace transactional-level detail is publicly available through a number of network-scanning technologies, such as Etherscan, although it is not necessarily structured in a user-friendly way. A token holder should consider identifying a diverse set of scanning technologies, particularly if holding digital assets from a lesser-known blockchain or a blockchain that implements privacy-preserving technology. Although the existence of privacy-enabling technology on blockchains likely increases the risk that digital assets are or have been used for illicit purposes, it can also impede a token holder's ability to accurately track balances and movement of funds.

Lastly, understanding the scope and nature of the validation checks performed on transactions by validating nodes is a good way to determine whether a network has a way to effectively screen potentially malicious transactions. At a minimum, look for rules that standardize transaction syntax, balance verification, provide digital signature validation and do not allow for abnormal or unconventional transactions.

8. In summary

The blockchain ecosystem is an incredibly complex mix of token holders, technological implementations and economic models that can be combined in a seemingly endless number of ways. Different types of token holders will have different risk appetites based on their use case for the asset. Technological blockchain designs and implementations are usually driven by operational requirements and the desire to solve the blockchain trilemma problem and largely have fallen short in this regard. This has led to a diverse ecosystem of application-specific chains with complex token ecosystems built atop, creating multilayered risk profiles that are, in most cases, completely unique. Understanding how all the layers interact and the risk trade-offs that exist as a result are nontrivial tasks, even for the crypto savvy. The pillars of risk and the criteria discussed are not exhaustive nor were they developed with one particular entity or blockchain in mind.

Our paper is designed to provide an agnostic framework based on components that are very likely to be applicable to all blockchains and the tokens that exist within them. The intention is to arm potential token holders, regardless of use case, with a guide on where to start and how to think about token risk across the entire ecosystem.

The framework cannot predict the performance or popularity of a particular token. The framework does not weigh the probability of a black swan event or the magnitude of its potential impact. However, using the framework may help in flagging potential exogenous and endogenous risks to protocols and, by affiliation, their tokens allowing prospective token holders to better understand the risks involved. Therefore, pairing the general framework with a technical risk and compliance assessment may produce the best results.

The framework can be useful for an inclusive set of participants, such as institutional investors, sell-side banks and dealers, and crypto-native institutions of various types.

9. How we can help

Ernst & Young LLP was a first mover in providing services to digital asset clients and has developed a cohesive, integrated approach to serving this market. We have brought together the capabilities of our global blockchain technology team with our time-tested solutions to build a dedicated digital asset practice for financial services. This extends our distinction as the only professional services firm with a dedicated financial services practice across assurance, tax, strategy and transactions, and consulting services, and positions us to help build, connect and protect participants in the digital asset ecosystem.

Our experience spans the development of the most foundational elements of digital asset strategy to the implementation of operating models, technology solutions and risk management frameworks. We support both traditional finance and digital-native organizations on topics ranging from blockchain engineering, technology and cybersecurity, to tax, finance, accounting, risk and regulatory compliance. On the regulatory front, we support clients that are in the early stages of designing and developing their products and preparing to engage with regulators, through the application process, go-live preparation and post-launch as firms go through exams and remediation exercises.

Our integrated digital assets team helps to build blockchain and digital asset solutions and actively supports clients in building a scaled and sustainable ecosystem.

References

1 "State of Compound Q1 2022," *Messari website*, messari.io/report/state-of-compound-q1-2022, 15 April 2022.

2 "Quantifying Decentralization," *news.earn.com website*, news.earn.com/quantifying-decentralization-e39db233c28e, 27 July 2017.

3 "Nakamoto Coefficient," *CrossTower website*, crosstower.com/resources/education/nakamoto-coefficient/?msclkid=16513b38c59611ec807d26d7e083bb04, accessed January 2023.

4 "Vitalik Sounds Alarm on Security of Cross-chain Bridges." *Yahoo Finance website*, www.yahoo.com/video/vitalik-sounds-alarm-security-cross-120031414.html, 11 January 2022.

5 "Wormhole Bridge Exploit Incident Analysis," *Certik website*, www.certik.com/resources/blog/1kDYgyBcisoD2EqiBpHE5l-wormhole-bridge-exploit-incident-analysis, 1 August 2022.

6 "Jump Trading Backstops Wormhole's $320M Exploit Loss," *CoinDesk website*, www.coindesk.com/business/2022/02/03/jump-trading-backstops-wormholes-320m-exploit-loss-sources, 3 February 2022.

7 "Issue #60: Juno Whale," *30,000 Feet website*, 30000feet.substack.com/p/issue-60-juno-whale, 20 March 2022.

8 "What are Smart Contracts?" *Blockgeeks website*, blockgeeks.com/guides/smart-contracts, 19 October 2022.

9 "DeFi dashboard," *DefiLlama website*, defillama.com, accessed January 2023.

10 "Solidity vs Vyper," *QuickNode website*, www.quicknode.com/guides/smart-contract-development/solidity-vs-vyper, 23 September 2022.

11 "What is Solidity Programming Language?" *Decrypt website*, decrypt.co/resources/solidity, 24 January 2019.

12 "Solidity Security: Comprehensive list of known attack vectors and common anti-patterns," *Sigma Prime website*, blog.sigmaprime.io/solidity-security.html, 30 May 2018.

13 "Compare Crypto Loan Platforms for Borrowing Against Crypto 2022," *DeFi Rate website*, defirate.com/borrow, 6 October 2022.

14 "Crooks steal $182 million from Beanstalk DeFi platform," *Cybersecurity World Conference website*, cybersecurityworldconference.com/2022/04/19/crooks-steal-182-million-from-beanstalk-defi-platform, 19 April 2022.

15 "EIP-1559: Fee market change for ETH 1.0 chain," *Ethereum Improvement Proposals website*, eips.ethereum.org/EIPS/eip-1559, 13 April 2019.

16 "Uniswap Grants Program," *Unigrants website*, www.unigrants.org, 2021.

17 "What is Tokenomics?" *Decrypt website*, decrypt.co/resources/tokenomics, 16 January 2019.

18 "Bitcoin Halving," *CoinWarz website*, www.coinwarz.com/mining/bitcoin/halving, accessed January 2023.

19 "Rewards and Penalties on Ethereum 2.0 [Phase 0]," *Consensys website*, consensys.net/blog/codefi/rewards-and-penalties-on-ethereum-20-phase-0, 2 March 2020.

20 "Ultra sound money," *ultra sound money website*, ultrasound.money, accessed January 2023.

21 "Terra Money: Stability and Adoption," assets.website-files.com/611153e7af981472d8da199c/618b02d13e938ae1f8ad1e45_Terra_White_paper.pdf, April 2019.

22 "SEC Chairman Jay Clayton: Cryptocurrencies Like Bitcoin Are Not Securities," CNBC, YouTube website, www.youtube.com/watch?v=8YtZJRUak8E, 6 June 2018.

23 https://decrypt.co/140247/sec-head-gary-gensler-insists-crypto-rules-are-already-clear.

24 https://www.reuters.com/legal/us-judge-says-sec-lawsuit-vs-ripple-labs-can-proceed-trial-some-claims-2023-07-13/.

25 DeFi Money Market Compound Overpays Millions in COMP Rewards in Possible Exploit; Founder Says $80M at Risk," CoinDesk website, ADD WEBSITE from footnote 25, updated 11 May 2023.

Authors

Mark Vangeloff
Blockchain Technology Consulting
Ernst & Young LLP
mark.vangeloff@ey.com

Matt McConnell
Digital Asset Business Consulting
Ernst & Young LLP
matthew.mcconnell@ey.com

Contributors

Steve Beattie
Financial Services Digital Assets Risk Leader
Ernst & Young LLP
steven.beattie@ey.com

Paul MacIntosh
Financial Services Digital Assets Leader
Ernst & Young LLP
paul.macintosh@ey.com

David Byrd
Blockchain Strategy Leader for Assurance
Ernst & Young LLP
david.byrd@ey.com

Mark Nichols
Capital Markets Digital Assets Strategy Lead
Ernst & Young LLP
mark.nichols@ey.com

Rebecca Carvatt
Banking and Capital Markets
Digital Assets Consulting Leader
Ernst & Young LLP
rebecca.carvatt@ey.com

Kristina Sanger
Financial Services Digital Assets
FinCrime Leader
Ernst & Young LLP
kristina.sanger@ey.com

Michael Gonzales
Financial Services Digital Assets
Assurance Lead
Ernst & Young LLP
michael.t.gonzales@ey.com

Chen Zur
US Blockchain Practice Leader
Ernst & Young LLP
chen.zur@ey.com

Arwin Holmes
Global Blockchain Chief Technology Officer,
Americas Consulting Metaverse Leader
Ernst & Young LLP
arwin.holmes@ey.com

Aaron Stafford
Financial Services Digital Asset
Blockchain Consulting
Ernst & Young LLP
aaron.stafford@ey.com

Brendan Maher
Financial Services Digital Assets Strategy
Ernst & Young LLP
brendan.maher@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2024 Ernst & Young LLP.
All Rights Reserved.

US SCORE no. 22465-241US_2
2401-4417859
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com