Venture Capital in Blockchain and Crypto

Evolution, Instruments, Governance, and Networks

Marta Zava

December 2025

marta.zava@unibocconi.it, Finance, SDA Bocconi, Milan. The author thanks Cristiana Muré for the precious contribution in the data collection and manuscript preparation

Table of Contents

1. Executive Summary

1.1 Key Findings

- Crypto venture capital now accounts for ~5% of global VC activity in 2025, with $6B invested in Q1 followed by a sharp drop in Q2, reflecting ongoing volatility.
- The sector is shifting from speculative early-stage bets to later-stage infrastructure and security investments, indicating growing operational maturity.
- Token-only, equity-only, and hybrid investment structures are not interchangeable: each defines different pathways of influence, enforceability, and value realization.
- Governance models (from cap tables to DAOs) increasingly determine not only who controls protocols, but also how legitimacy is perceived by communities.
- Regulatory frameworks such as the EU's MiCA and the U.S. GENIUS Act bring long-awaited clarity to stablecoin and CASP regulation, though significant gaps remain in DeFi, DAO liability, and token classification.

1.2 Contributions of the Report

- Provides a typology of crypto VC instruments and analyzes how deal structures shape investor power, founder alignment, and strategic outcomes (Section 6).
- Examines governance regimes across centralized and decentralized ecosystems, highlighting how VCs exert soft and hard power (Section 7).
- Offers data-driven insights into the state of crypto VC in 2025, including deal volumes, investment stages, geographic shifts, and category allocations (Section 4).
- Synthesizes regulatory developments in the EU and U.S., comparing legal approaches to reserve backing, licensing, redemption, and insolvency treatment (Section 5).
- Connects financial capital flows with institutional and governance infrastructures, bridging investment practice and policy relevance.

1.3 Policy & Industry Implications

- **For policymakers**: The priority is now to build globally interoperable frameworks that cover not just stablecoins and CASPs, but also DeFi protocols and DAOs, without stifling innovation.
- **For investors**: Competitive advantage lies in mastering new instruments (e.g. SAFTs, token rights, DAO delegation) and participating in governance, not just sourcing deal flow.
- **For founders**: Capital partners and deal design define long-run viability: token design, governance rights, and investor reputations shape community trust and regulatory exposure.
- **Across the board**: Institutionalization, not ideology, will determine whether crypto is entering a stable growth phase or heading toward a deeper structural winter.

2. Crypto VC at a Glance

2.1 Timeline of Crypto VC, 2012–2025

2012-2013: Early VC Entry. Venture capital entered crypto cautiously, raising just $2.1 million in 2012. The first significant wave of institutional VC interest in Bitcoin startups occurred in 2013, when Coinbase, Circle, and BTC China received support from leading companies like a16z and Lightspeed.

2014-2015: Expansion of Bitcoin Applications. Emerging as the most active investment firm, 500 Startups supported Bitcoin application startups alongside Plug and Play Technology Centre, Boost VC, and CrossCoin Ventures. After initially concentrating on the cryptocurrency space, 500 Startups eventually moved to more general early-stage investments, paying less attention to crypto payments and transactions. Despite BTC's price slump, blockchain funding hit $380M in 2015, showing sustained VC conviction.

2016: Shift to ICO. As fintech investment decreased, venture capital investment in the cryptocurrency business followed the same trend. CB Insights reports that investments in blockchain and Bitcoin firms fell 27% from 2015 levels, reaching 2014 levels. Meanwhile, ICO-based project funding started to expand; the ICO boom began when The DAO raised $150 million.

2017: ICO and Tokenomics Raise. New funds like Polychain, MetaStable, and Multicoin Capital shifted from traditional equity models to liquid, token-based strategies. Pantera Capital launched its ICO Fund in 2017, targeting ICOs and token projects, while Blockchain Capital introduced the BCAP token, a security token representing a share in their fund. Ethereum's ERC-20 fueled massive growth, while regulatory scrutiny set the stage for a bear market. ICOs raised $5 billion across nearly 800 projects, five times the $1 billion VC investment in 215 transactions.

2018: Scaling the Investment. ICO activity peaked with 1253 projects raising $7.8B, as reported by CoinSchedule. Meanwhile, VCs funded major players like Bitmain ($1B+ pre-IPO), with total VC crypto funding at $4.26B, showing parallel growth of equity and token financing.

2019-2020: Stabilization and Rise of DeFi. VC funding stabilized in 2019 with 622 deals worth $2.75B, giving blockchain 2.8% of all VC deals and showing growing institutional interest. By 2020, over 942 VCs had backed 2,700+ blockchain startups, and top crypto funds were consistently outperforming traditional VC. Although still under 1% of global VC, blockchain private equity was becoming a credible asset class. Meanwhile, DeFi gained traction, drawing $280M in funding and dominating deal counts, signaling the rise of crypto-native finance.

2021: Golden Year. Crypto VC hit an all-time high around $30B raised across 2,000+ deals. The increase in late-stage financings caused 65 startups to became unicorns, and traditional giants like Morgan Stanley, Sequoia, Samsung, and Goldman Sachs entered the blockchain market through late-stage equity investments, contributing to a market flush with capital. This was crypto's mainstream VC breakout.

2022: Peak and Collapse. Crypto VC investment peaked at $30B+, concentrated in later-stage deals. However, the FTX collapse wiped out billions, with Sequoia Capital writing down its $200 million investment to zero, and Temasek's $320 million worth of FTX shares becoming worthless. Web3 led deal counts, while trading platforms attracted the most capital. Despite the boom in the first half of the year, valuations fell to their lowest since early 2021, marking the end of the virtuous cycle.

2023-2024: Winter. With deal sizes and valuations near 2020 lows, funding fell to just one-third of previous years in 2023. While pre-seed decreased, early-stage activity predominated. By 2024, crypto VC activity had gradually increased, reaching $3B in Q2 and growing for three consecutive quarters. The biggest investment went to AI, although Web3 remained a top priority.

2025: A Mature Runup. Due to Binance's $2 billion round, funding soared over $6 billion in Q1 before cooling to about $2B in Q2. For the first time federal crypto legislation was passed by US politicians, establishing standards for stablecoins. Circle prepared for IPO, a milestone after Coinbase's 2021 listing. Funding was driven by mining, security, and infrastructure, and later-stage investments exceeded early-stage deals, indicating a mature, regulated sector.

3. Introduction

Why is this study relevant now?

Over the past decade, crypto assets have matured from fringe experiments to investable technologies with real-world applications, global developer communities, and institutional capital inflows. What was once dismissed as speculative or ideologically radical now commands the attention of sovereign funds, Tier 1 venture capital firms, and financial regulators alike. This report examines the changing face of venture capital in crypto (how VCs invest, govern, and adapt to tokenized economies) and why understanding these dynamics is increasingly urgent.

Venture capital investment in blockchain and crypto-related companies now accounts for roughly 5% of global VC flows, a share that was nearly negligible ten years ago. More striking than the absolute figure is the persistence of this allocation across market cycles. Unlike the boom-and-bust pattern seen in retail-driven crypto markets, VC interest in the sector has demonstrated structural resilience: even in years marked by price crashes or regulatory pressure, funding volumes have stabilized, and many large players have doubled down. The steady allocation in crypto-related VC deployment is not simply a story of hype, but of long-term capital formation across infrastructure, applications, and financial primitives. (See Section 4: An Empirical Overview)

Moreover, the allocation between early-stage and late-stage rounds has become evenly split, roughly 50/50, a feature that signals the maturation of the ecosystem. Early-stage investments continue to drive experimentation and protocol design, while later-stage deals support scaling infrastructure, institutional services, and regulatory compliance. The presence of both reflects a rare convergence: a venture market that remains exploratory in its frontiers, but increasingly institutionalized in its core. In this duality, crypto is not merely a new asset class: it is becoming a new investment logic. (For a breakdown of financing structures, see Section 6: How Do VCs Invest?)

Together, these developments place us at a transitional moment: where crypto-native innovation and traditional venture capital no longer operate on parallel tracks, but instead negotiate governance, incentives, and power within increasingly convergent systems. This report maps the instruments, legal architectures, and network strategies through which this convergence is taking place.

How do venture capitalist invest?

In traditional venture ecosystems, the structure of investment is governed by a familiar and relatively standardized toolbox: equity rounds, convertible notes, board representation, and a clear path toward exit via acquisition or listing. In the blockchain space, however, the mechanics of investment have undergone a profound transformation. Venture capitalists are no longer investing solely in companies, but also in protocols, tokens, and decentralized communities. This shift has introduced new instruments, blurred legal boundaries, and created novel tensions between financial backing and participatory governance. Understanding how VCs deploy capital in crypto is thus essential not only for assessing risk-return profiles, but for mapping the evolving architecture of digital markets.

In a subset of blockchain-related ventures, particularly those offering custodial services, analytics infrastructure, or enterprise-grade tooling, the dominant investment mode remains equity-only. These firms operate as conventional corporations with no immediate plans to issue native tokens or decentralize governance. In such contexts, capital is deployed through convertible instruments, SAFEs, or priced equity rounds, often replicating the contractual structures of traditional startup finance. Yet even here,

the boundaries are becoming increasingly porous. Equity rounds in crypto-native ventures are frequently negotiated alongside side letters or token warrants, creating hybrid claims on future digital assets that are not captured on the cap table. At early stages, when the business model and token design are still evolving, investors often accept legal ambiguity in exchange for strategic optionality. This produces a paradox: while equity instruments offer the greatest legal protection, their value may ultimately depend on future token outcomes that are neither guaranteed nor formally linked. The implications of this shifting terrain are discussed further in Section 6.1.

A second, and increasingly prominent, category involves token-only investments. Here, venture capitalists commit capital in exchange for future or circulating tokens, without acquiring any formal equity stake. These deals are typically structured through SAFTs (Simple Agreements for Future Tokens), direct token purchases, or allocations negotiated with DAO treasuries. Unlike equity, tokens are liquid, programmable, and may confer governance rights within decentralized protocols. However, they offer no guaranteed control, no board oversight, and little legal recourse. While these characteristics may align with the ethos of decentralization, they also introduce significant volatility, regulatory uncertainty, and reputational risk. For instance, tokens acquired at early stages may become tradeable far before a protocol reaches maturity, prompting criticism of short-term behavior by institutional holders. The dynamics and limitations of this approach are analyzed in Section 6.2.

In practice, a growing number of high-profile deals combine both equity and token exposure. These hybrid structures are now common among leading protocols, including Uniswap, dYdX, Axie Infinity, and Arbitrum. Venture investors receive equity in the operating company (or lab), alongside token allocations that provide governance rights or access to economic upside in the underlying protocol. In principle, hybrid deals offer the best of both worlds: enforceable legal claims on corporate value, and strategic influence over decentralized infrastructure. In reality, they are often legally complex and structurally fragile. Timing mismatches between the liquidity of tokens and the illiquidity of equity can create divergent incentives among investors and founders. Dual governance systems, one centered on a corporate board, the other on a DAO, can generate conflicts over priorities, disclosure, or control. The legal frameworks underpinning these arrangements are not standardized, and the scope for regulatory scrutiny or community backlash remains high. The strategic, legal, and incentive challenges of these models are explored in Section 6.3.

Ultimately, the distinction between equity-only, token-only, and hybrid venture capital structures is not a matter of legal form alone. It determines the locus of investor control, the enforceability of rights, and the distribution of upside across both corporate and protocol layers. These design choices are not neutral: they influence how projects are governed, how contributors are incentivized, and how communities perceive legitimacy. While some investors treat these instruments as interchangeable wrappers for financial exposure, the structural configuration of a deal often embeds assumptions about power, liquidity, and exit paths. Understanding these implications is essential for founders, funds, and policymakers alike.

Yet the boundaries between categories are increasingly porous, and at times strategically ambiguous. SAFEs contain side letters promising future tokens; equity rounds embed token warrants or parallel claims on protocol treasuries; token allocations are subject to vesting enforced by smart contracts rather than courts of law. These hybrid configurations raise critical legal and institutional questions. Can side letters for future tokens be enforced if the issuing protocol is governed by a DAO rather than a company? Can a DAO vote reverse a treasury deal negotiated off-chain? How should regulators interpret a deal where formal legal rights are minimal, but influence is exercised via token accumulation or delegated governance? These tensions underscore the fragility of contractual design in a rapidly evolving legal landscape.

As the crypto venture capital ecosystem continues to mature, the architecture of investment instruments will shape more than individual deals: it will define the institutional grammar of web3 itself. The risks, constraints, and governance implications of these choices are not merely theoretical: they are playing out in real-time across token treasuries, governance forums, and decentralized financial networks. For a deeper investigation of these structures, including the incentives they create, the conflicts they generate, and the innovations they enable, see Section 6 of the report.

Who governs the protocols?

While much of the attention in blockchain venture capital has focused on financial engineering and deal structuring, the more enduring challenge lies in governance. In an ecosystem defined by decentralization, programmability, and collective coordination, the way decisions are made (about protocol upgrades, treasury disbursements, or ecosystem incentives) is not a peripheral matter. It constitutes the core institutional architecture of Web3. As venture capital becomes increasingly embedded in this architecture, a pressing question emerges: how are governance models in crypto designed, captured, or resisted, and what role do financial actors play in shaping their evolution?

The early promise of token-based governance was radical and compelling: an open system where decision-making rights would be distributed proportionally to token holders, enabling scalable, permissionless participation. This "one token, one vote" mechanism mirrored shareholder models but operated natively on-chain. Yet in practice, token governance has revealed deep structural fragilities. Token allocations are often heavily concentrated in the hands of insiders and early investors. Voter turnout remains stubbornly low, coordination costs are high, and accountability mechanisms are weak. The result is a system where formal decentralization often masks informal centralization, particularly in the hands of venture capital funds with significant token holdings. As analyzed in Section 7.1, this governance asymmetry has not only strategic but legitimacy consequences, raising concerns about the resilience and credibility of DAOs in the face of concentrated influence.

Perhaps no episode illustrates these dynamics more vividly than the case of a16z's involvement in Uniswap governance. In 2021, a governance vote to deploy Uniswap on BNB Chain was opposed by a16z. They did not do it directly, but through a network of university blockchain clubs to which it had delegated its UNI tokens. The delegation strategy avoided explicit control while maintaining effective influence, particularly given the proposal's implications for LayerZero, a16z's portfolio company. This incident, discussed in detail in Section 7.1.3–7.1.4, exemplifies a broader pattern in which VCs exert soft power via token delegation, forum coordination, and meta-governance tooling, blurring the boundary between active stewardship and covert capture.

These strategic behaviors have prompted a wave of design responses across the ecosystem. Protocols have begun to implement resilience mechanisms: procedural constraints such as vesting schedules, quorum thresholds, timelocks, and proposal queues intended to prevent abuse and foster transparency. Yet these institutional safeguards remain limited in scope, often reactive rather than systemic. As argued in Section 7.1.4, the deeper problem may lie not in voting rules but in governance token design itself. Should voting power be strictly proportional to capital? Should tokens be transferable, or instead soulbound and reputation-based? Should influence accrue from past contributions rather than present holdings? These questions are increasingly central to both academic and policy debates about DAO governance legitimacy.

What emerges from these developments is a growing recognition that governance in crypto is not a monolith, but a multidimensional design space. Protocols like Optimism, for example, have embraced bicameral governance, introducing a dual structure with a Token House and a Citizens' House, each representing different sources of legitimacy (economic and reputational, respectively) (Section 7.3.3).

Others, such as Polkadot and Curve, rely on conviction voting and vote-escrow models, where influence is tied to time commitment and staking behavior rather than sheer token quantity (Section 7.3.1–7.3.2). These alternative mechanisms attempt to realign incentives and resist sybil manipulation, albeit with varying degrees of success.

At the opposite end of the spectrum, some ecosystems reject token governance altogether. Hedera Hashgraph, for instance, is governed by a council of global enterprises with equal voting rights and identifiable fiduciary responsibilities. This non-token governance model, discussed in Section 7.2, emphasizes legal accountability and long-term stability over openness and permissionless participation. While attractive to institutional actors and regulators, such models risk alienating the broader Web3 community, raising important questions about inclusiveness, adaptability, and ideological coherence.

Governance-by-code represents a further trajectory in the search for credible commitment. Protocols like Stacks, which embed rules directly into smart contracts, aim to minimize discretionary decision-making altogether, replacing human governance with deterministic processes (Section 7.3.6). Meanwhile, projects such as Gitcoin and Radicle explore quadratic voting, identity-weighted participation, and contribution-based reputation systems, attempting to engineer legitimacy from a more pluralistic and participatory foundation (Section 7.3.4–7.3.5). These efforts speak to a deeper philosophical debate: is decentralization a property of infrastructure, or a process of ongoing negotiation among stakeholders?

A comparative reading of governance implementations across leading protocols (Uniswap, Compound, Arbitrum, Optimism) suggests that no single architecture offers a definitive solution. As examined in Section 7.4, each model navigates a different balance of trade-offs: between efficiency and inclusion, transparency and complexity, legitimacy and control. What distinguishes effective governance is not its conformity to an ideal type, but its responsiveness to the strategic, technical, and social realities of its ecosystem.

What's Going On in 2025?

The year 2025 may be remembered either as the foundation of crypto's mature expansion, or as the prelude to a prolonged stagnation. After a bruising reset triggered by the 2022 FTX collapse, venture capital flows into crypto rebounded sharply in early 2025, only to retreat just as abruptly in the following quarter. This volatility, while partly driven by idiosyncratic deals such as Binance's $2 billion raise, underscores a broader structural uncertainty: investors, protocols, and policymakers are navigating a fragile equilibrium between renewed optimism and the memory of systemic failures.

The data show both resilience and tension. Crypto startups raised $6 billion in Q1 2025, more than double the previous quarter, with stablecoins gaining $25 billion in circulation and infrastructure security deals surging after the Bybit hack. Yet by Q2, funding dropped nearly 60%, deal count fell by 15%, and late-stage rounds overtook early-stage activity for only the second time in four years. This suggests not merely cyclical fluctuation, but a shift in investment philosophy: from experimentation to consolidation, from token narratives to enterprise resilience. Exit markets, too, hang in the balance. Circle's pending IPO may provide the first real price-discovery event since Coinbase's 2021 listing, while the broader pipeline remains uncertain. In Section 4 we propose a complete breakdown of capital flows, deal stage dynamics, sector allocation, and geographic concentration.

On the legislative front, 2025 is also a watershed year. For the first time, two major jurisdictions, the United States and the European Union, have introduced comprehensive regulatory frameworks that move beyond enforcement toward proactive rulemaking. The GENIUS Act in the U.S. offers a blueprint for stablecoin oversight, full-reserve requirements, and priority creditor rights. MiCA in the EU

establishes a horizontal regime for crypto-assets, integrates stablecoins into prudential regulation, and mandates disclosures across issuers and service providers. While differing in scope and philosophy, both frameworks lay a foundation for institutional re-entry and cross-border compliance. At the same time, they expose gaps around DeFi, DAOs, and token classification, the very spaces where innovation is accelerating. Section 5 offers a comparative analysis of the unresolved tensions they leave behind.

What's next?

In 2025, crypto venture capital stands at a pivotal inflection point. The speculative surges of previous cycles have given way to a more discerning, often ambivalent, investor environment: one in which capital no longer chases mere narratives but demands institutional-grade robustness. The ability of crypto startups to attract long-term investment will now depend less on whitepapers and token velocity, and more on the maturity of their operational models, the legal clarity of their instruments, and the integrity of their governance frameworks. These are not ancillary concerns but prerequisites for legitimacy in a system still struggling to define its place in global finance.

The landscape ahead is not devoid of opportunity. Legislative progress on both sides of the Atlantic, with the EU's MiCA and the U.S. GENIUS Act, offers, for the first time, the contours of a stable regulatory perimeter. At the same time, funding activity, while volatile, continues to support infrastructure, security, and scaling solutions, suggesting that institutional interest has not evaporated, but merely recalibrated. What is emerging is not the next hype cycle, but the slow construction of an investable asset class: one in which regulatory compliance, technical auditability, and credible decentralization co-exist as foundational pillars.

Whether this moment becomes the beginning of crypto's long institutional trajectory or the onset of a deeper structural winter will depend less on short-term capital flows and more on the institutional architecture being shaped in real time: by investors, policymakers, and protocol designers alike. Sustainable crypto venture capital will require more than bold engineering; it will rest on credible mechanisms for enforcement, scalable governance, and coherent regulatory interfaces. What is at stake is not just the future of a technology, but the emergence of a new asset class capable of withstanding volatility, earning trust, and integrating meaningfully into the broader financial system.

4. From Inception to Today – An Empirical Overview

The evolution of venture capital in crypto mirrors the broader trajectory of the industry itself: from the launch of Bitcoin's whitepaper and Ethereum's smart contracts, to the ICO boom, the rise of token-focused funds, the DeFi summer, and the disruptive ("recovered") collapse of FTX. Each stage brought new technological milestones, funding models and shifts in investor sentiment. What began as a niche experiment has grown into a global asset class, shaped by cycles of innovation, speculation, crisis and regulation. This section traces the defining moments and investment patterns from crypto's origins to today's more institutionalized landscape.

4.1. Defining Moments

4.1.1 The very beginning: Bitcoin Whitepaper

In October 2008, the publication of "Bitcoin: A Peer-to-Peer Electronic Cash System," written under the pseudonym Satoshi Nakamoto, marked the beginning of the revolution in traditional digital commerce. Bitcoin's whitepaper proposed an alternative to digital payments which based its structure on cryptographic proof rather than trust, enabling any two willing parties to conduct business directly with one another without the assistance of an outside entity. The project began with the adoption of the standard structure of digital signature-based coins, which offered robust ownership control but was limited by the absence of a mechanism that prevented double-spending. This was resolved by proposing a peer-to-peer network that uses proof-of-work to record a public history of transactions. Making computationally prohibitive for an attacker to alter this history if honest nodes control a majority of CPU power. The network's unstructured simplicity then contributes to it robustness (Nakamoto, 2008).

Fast forward to January 2009, Bitcoin officially launched during the global financial crisis pushing forward the concept of a decentralized, blockchain-based digital currency and store of value. Institutional venture capital, however, paid little attention during these early phases. Professional cryptographers, individual enthusiasm, and a few angel investors were the driving forces behind Bitcoin's rise; typical venture capital funds stayed in the background. Only over $2 million in venture capital was given to Bitcoin startups overall in 2012. By comparison, that year's global venture capital investment was over $50 billion.

4.1.2 Overcoming existing limits: Ethereum ICO

From the incipit of the Bitcoin era, most of the subsequent cryptocurrencies were mostly variations of their ancestor. The real jump forward came with Ethereum, created to overcome Bitcoin's scalability limits and to enable programmable applications through smart contracts. While the first ICO was launched by Mastercoin in 2013, it was Ethereum's own Initial Coin Offering in 2014 that revolutionized the fundraising model for blockchain projects, with its innovation laying in its own infrastructure.

Through its smart contracts, and especially the introduction of the ERC-20 token standard, Ethereum became the easiest platform to create and distribute new tokens. As a result, most ICOs were conducted in exchange for Ether (ETH), firmly establishing Ethereum as the base of the emerging token economy. This flexibility also enabled the development of decentralized applications (dApps) and laid the foundations for what would later become decentralized finance (DeFi).

Initial coin offerings (ICOs) have emerged as a new mechanism for entrepreneurial finance, with parallels to initial public offerings, venture capital, and pre-sale crowdfunding. (Howell et al., 2018). As Fenu et al. (2018) study notes, *"the vast majority of ICOs came to rely on Ethereum's ERC-20 token standard, which enabled developers to clone smart contracts and issue tokens with minimal technical effort. This lowered the barrier to entry, fueling the exponential rise in token launches and speculative investment."* Thus, Ethereum's 2014 ICO not only financed

the development of the protocol itself but also provided the technical and financial framework that powered the ICO boom of 2017.

4.1.3 Increasing interest: the first institutional token round

Driven by the ICO boom and interest in tokenized assets, the VC environment for liquid crypto investments started to take shape with the emergence of institutional token rounds. Not just stocks but tokens were now the focus of early funds like Polychain Capital and MetaStable Capital. While Blockchain Capital introduced the BCAP token, a security token that represented a part in their fund, Pantera Capital established its ICO Fund in 2017 with an emphasis on ICOs and token projects. Token investments were also emphasised by Multicoin Capital and 1confirmation. Amentum Investment Management joined in 2017 with the goal of investing in token-based economies and blockchain technology for long-term capital growth.

These funds switched from conventional equity models to the inclusion of liquid, token-based strategies after realising the potential of tokenised assets, structuring their deals in a hybrid mode that combined holding equity in a company with the rights to future tokens. From this followed the realization that tokens were no longer a retail phenomenon, but a new asset class attracting top-tier venture investors. Crucially, they also set the stage for dedicated crypto VC funds like a16z Crypto, a $350M venture fund launched in 2018 with the objective to make long-term investments in crypto companies and protocols. Legally these deals were often structured through SAFTs (Simple Agreement for Future Tokens), which are defined in their whitepaper as both an investment and a security: obligating investors to immediately fund developers in exchange for a genuinely functional network and, subsequently, tokens, on one side, but also consumpting products demanding compliance with the securities and consumer protection laws, on the other (Batiz-Benet et al., 2017).

4.1.4 DAOs and the DeFi summer

The rise of Decentralized Autonomous Organizations (DAOs) and the increasing interest in decentralized finance (DeFi) in 2020 marked a turning point in cryptocurrencies history. A DAO is an internet-native organization in which ownership and decision-making are distributed among token holders. Members control the organization collectively and in a decentralized way, by voting on proposals, such as which rules should be encoded in smart contracts or how treasury funds should be allocated. Tokens issued by DAOs can represent economic value, governance rights, or permissions, and are also used to reward community contributions. Overall, these entities rely on blockchain-based smart contracts to automatically enforce voting outcomes and to store transactions transparently, thereby aligning the interests and actions of participants toward a shared purpose (Ellinger et al., 2024).

In this same year total investment and financing in the encryption industry amounted to approximately $3.566 billion, comparable to the 2019 figures. DeFi projects received $280 million, accounting for 7.8% of the total. Despite the relatively small amount, DeFi had the highest number of financings, with over a quarter of the 407 disclosed projects being DeFi-related. All the signals are now pointing towards the relevant growth potential in this new type of crypto-native project, which will manifest itself more vividly in the "golden year" of crypto: 2021.

4.1.5 FTX collapse and investor retreat

While venture capitalists were consolidating their interest in the sector, with over $30 billion in crypto and blockchain startups invested in 2022, FTX, a Bahama-based cryptocurrency exchange founded in 2019 set off a chain reaction that provided a noteworthy example of risk management failure. FTX's risk exposures were due to its heavy balance sheet reliance on illiquid, self-issued tokens such as FTT Token

(FTT) and Serum (SER), created by people involved with the creation of FTX and related companies such as Alameda Research. Therefore, the balance sheet reserves of these companies were directly influenced by tokens created and traded by FTX and dependent companies, through which the subsequent collapse (filing for bankruptcy in November 2022) has brought much of the industry into disrepute (Conlon et al., 2023).

Thus, investments peaked in the first half of the year and then faced significant drawdowns in Q3 and Q4, which experienced the lowest deal count and capital investment in two years. Prominent VCs who invested in FTX faced significant losses. Sequoia Capital wrote down its $200 million investment to zero, and Temasek's $320 million worth of FTX shares became worthless. The consequences were severe. In 2023, venture investment in crypto fell to roughly one-third of the levels seen in the previous two years, with deal count and capital invested hitting new lows each quarter. Fundraising for new funds became increasingly difficult, as limited partners, already cautious due to macroeconomic conditions, recoiled from the reputational damage caused by FTX.

4.1.6 The regulation era: the return of institutional capital

The collapse not only froze capital flows but also accelerated regulatory efforts worldwide, with policymakers citing FTX as evidence of the systemic risks posed by obscure governance and self-referential token economies. Indeed, these years of regulatory ambiguity were followed by a new era of institutional re-engagement with crypto, driven by regulatory frameworks aimed at providing clarity and a first basis for the integration of crypto into global finance.

In addition to freezing financial flows, the collapse sped up global regulatory efforts, with policymakers pointing to FTX as evidence of the systemic risks that self-referential token economies and obscure governance represented. Indeed, these years of regulatory ambiguity were followed by a new phase of institutional re-engagement with cryptocurrency, encouraged by regulatory frameworks intended to offer not only clarity but also a foundation for the integration of cryptocurrency into global finance.

4.1.7 FTX: Not everything was lost

Although the collapse of FTX in late 2022 dealt a severe blow to investors and the broader crypto ecosystem, the aftermath has shown that not all capital was permanently lost. Thanks in large part to blockchain transparency and aggressive recovery efforts under the court-supervised bankruptcy process, a significant portion of assets has been traced, secured, and is being returned to creditors and former customers. As of recent estimates, the FTX estate has clawed back between roughly $14.7 billion and $16.5 billion in assets, a figure that includes cash, liquid crypto holdings, and other recoverable property (the recovered amounts often far exceeded initial projections and implyed overall recovery rates above 100 % for certain creditor classes once postpetition interest is considered.)

These recoveries have been facilitated by meticulous on-chain tracking of crypto movements, frozen issuances of stolen tokens (e.g., portions of stablecoins traced to unauthorized transfers), and legal actions to reclaim assets improperly moved before bankruptcy. Under the approved reorganization plan, distributions have already begun (including major payouts such as a ~$1.6 billion creditor distribution in late 2025) and many retail users are expected to recoup most, if not all, of their original balances (with priority classes potentially receiving more than 100 % of their claim value due to accrued interest and asset value appreciation).

This unfolding recovery narrative underscores a distinctive feature of blockchain-native systems: despite opaque governance failures at the organization level, the visible and immutable ledger has enabled unprecedented asset retracing and restitution efforts, setting a noteworthy precedent for risk management and creditor outcomes in decentralized finance crises.

4.2 A snapshot in numbers

While the historical milestones of crypto venture capital trace the sector's storyline, a clearer picture of its scale, volatility, and evolution is obtainable by tracing when, where and how much capital VCs decided to allocate when it came to crypto. From its modest beginnings in the early 2010s, crypto VC funding has become a multi-billion-dollar market embedded within global venture flows. The following figures highlight long-term trends, the boom-and-bust cycle around 2021-2023, the subsequent recovery in 2024-2025, and a breakdown of the activity by deal count and stage.

4.2.1 Global VC Funding vs. Crypto VC Funding

Yearly Total vs. Crypto VC Capital Invested

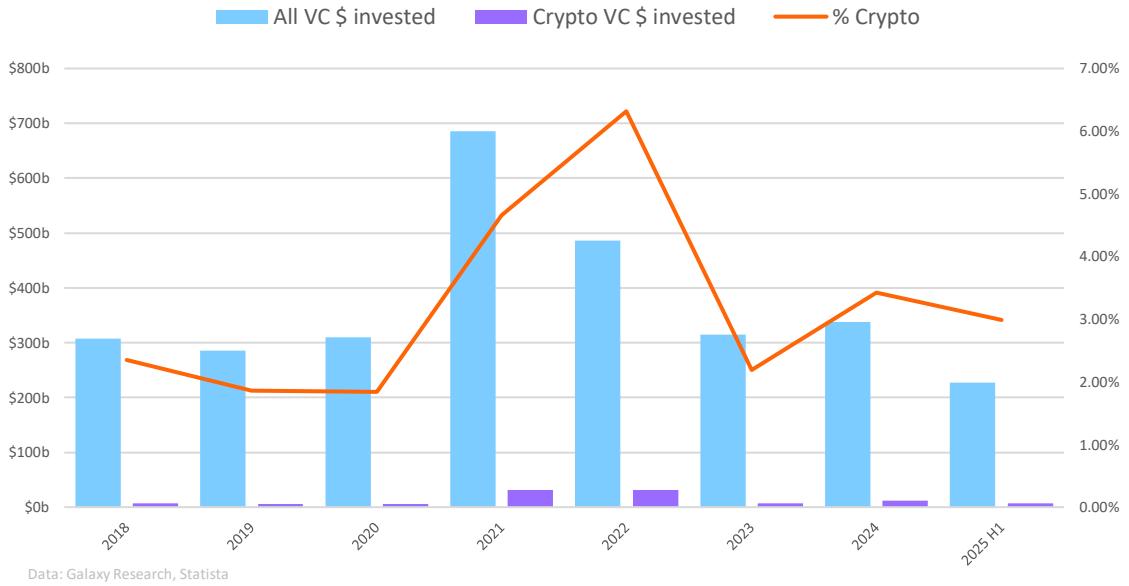

Figure 1. Yearly Total vs. Crypto VC Capital Invested. Annual global venture capital investment compared to crypto-specific VC, highlighting crypto share of total funding from 2018 to the first half of 2025. Source: Galaxy Research, Statista.

Between 2018 and 2020, crypto VC represented a small fraction of global VC activity, averaging around 2%. The boom years of 2021 and 2022 saw first absolute crypto investment and then relative share surge, with crypto's contribution peaking above 6% on average in 2022, the highest on record. The FTX collapse in late 2022 triggered a sharp contraction in 2023, pulling the share down to around 2%. While 2024 showed modest recovery, preliminary H1 2025 data suggests stabilization at roughly 3%, reflecting a cautious but renewed institutional engagement with the sector.

Quarterly Total vs. Crypto VC Capital Invested

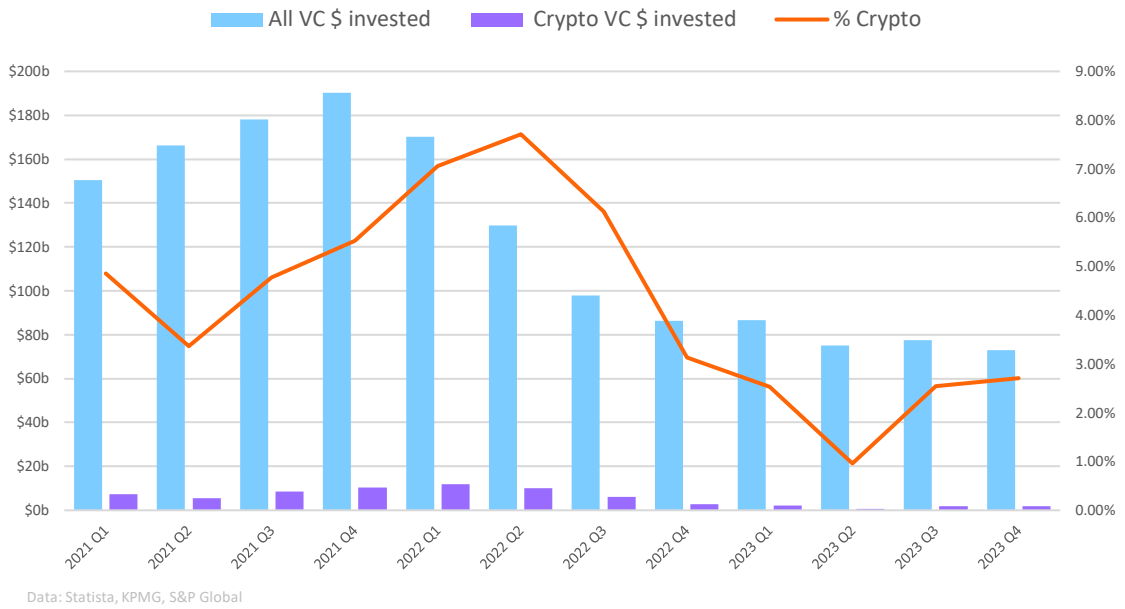

Figure 2. Quarterly Total vs. Crypto VC Capital Invested. Quarterly zoom-in, from 2021 to 2023, on global venture capital investment compared to crypto-specific VC. Sources: Statista, KPMG, S&P Global.

While absolute crypto VC investment peaked at over $30B in 2021, its share of global venture funding remained modest, orbiting around 4.5% that year. This share then reached its highest point in Q2 2022, just before the steep downturn, above 7% of total VC investments.

4.2.2 Zooming-In on Internal Volatility

Downturn and Recover of Crypto VC Investment

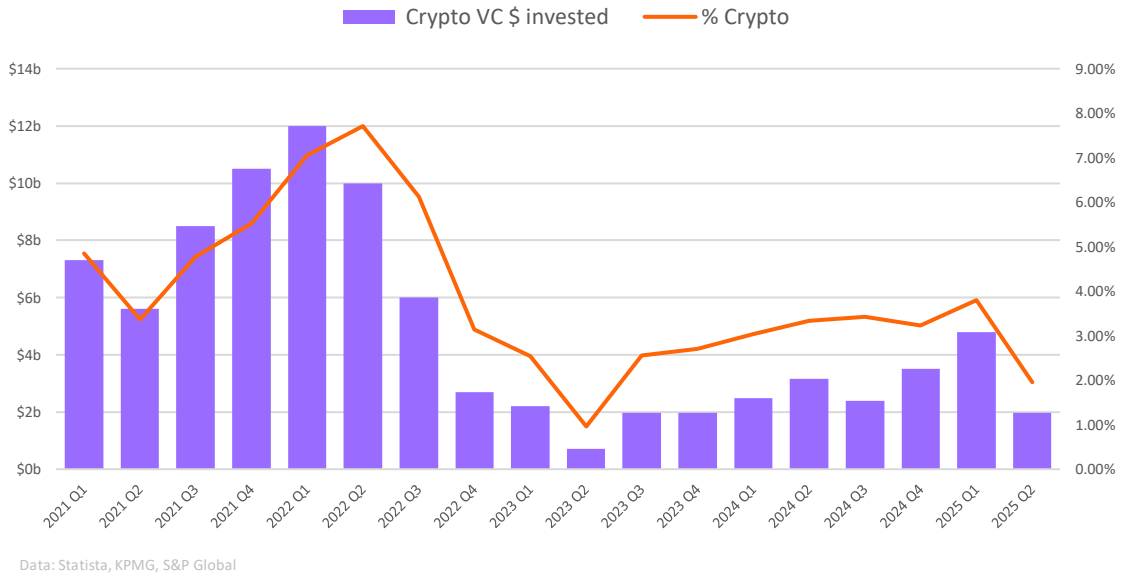

Figure 3. Downturn and Recover of Crypto VC Investment. Quarterly zoom-in on internal volatility, from 2021 to 2025, on the capital invested in crypto startups versus percentage share of total VC. Sources: Statista, KPMG, S&P Global.

Focusing specifically on crypto VC, Figure 3 shows the sector's internal volatility. After bottoming out below $1B in Q2 2023, funding gradually recovered through 2024, stabilizing in the $2-4B range per quarter. Early 2025 remains highly volatile: Q1 saw nearly $6B raised, boosted by Binance $2B minority investment, followed by a 59% contraction in Q2. These swings show both the fragility of deal flow and the continued willingness of investors to back large, strategic bets.

4.2.3 Capital Invested and Deal Count

Crypto VC Capital Invested & Deal Count

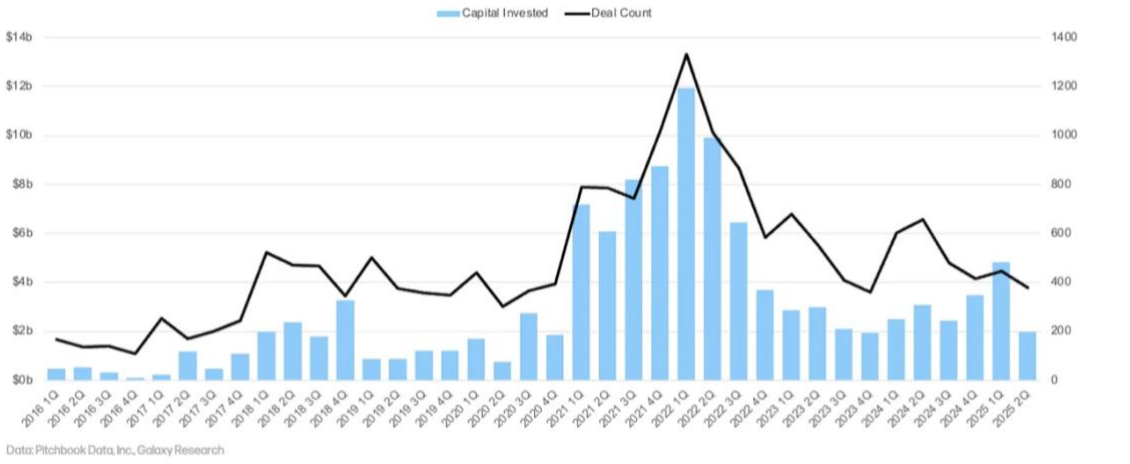

Figure 4. Crypto VC Capital Invested & Deal Count. Total Quarterly capital and number of deals in crypto VC from 2016 to 2025 Q2. Source: Pitchbook Data Inc., Galaxy Research.

The boom of 2021-2022 was broadly spread rather than limited to a handful of mega-deals: both capital invested and deal count surged, with quarterly activity peaking at more than 1,000 deals. The collapse of FTX in late 2022 then triggered a sharp contraction, cutting total capital to one-third of prior levels in 2023 and halving deal activity. By 2025, however, funding began to rebound under clearer regulatory regimes and renewed institutional participation, though with only ~400 deals per quarter as evidence of a more selective, disciplined investment environment.

4.2.4 Capital Invested by Stage

Crypto VC Capital Invested by Stage

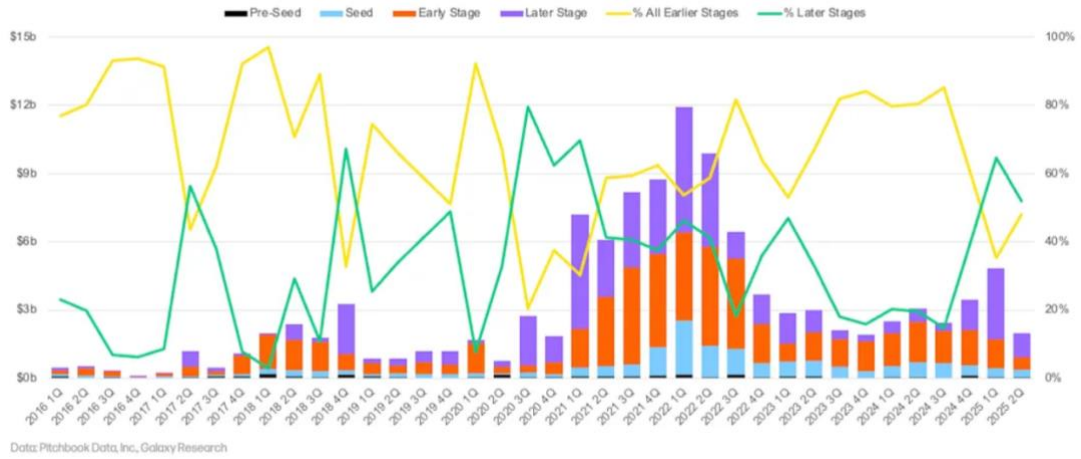

Figure 5. Crypto VC Capital Invested by Stage. Quarterly breakdown, from 2016 to 2025 2Q, of crypto VC funding by stage (pre-seed, seed, early stage, later stage), highlighting the respective share of earlier and later stages. Source: Pitchbook Data, Galaxy Research.

During the 2021-2022 frenzy, early-stage rounds dominated, reflecting speculative experimentation. In contrast, by Q2 2025, later-stage companies attracted 52% of total capital, marking only the second time since early 2021 that later-stage funding has overtaken early-stage activity. This shift suggests a preference for scaling proven models rather than backing new experimental ventures, reflecting the gradual institutionalization of the sector.

4.2.5 Capital Invested and Deal Count by Geography

In Q2 2025, 47.8% of capital invested went to companies headquartered in the United States. The United Kingdom was second with 22.9%, followed by Japan with 4.3%, and Singapore with 3.6%. Similar percentages are reported for deal count, displayed in Figure 6.

Crypto VC Deals in Q2 2025 by Startup Headquarters Country

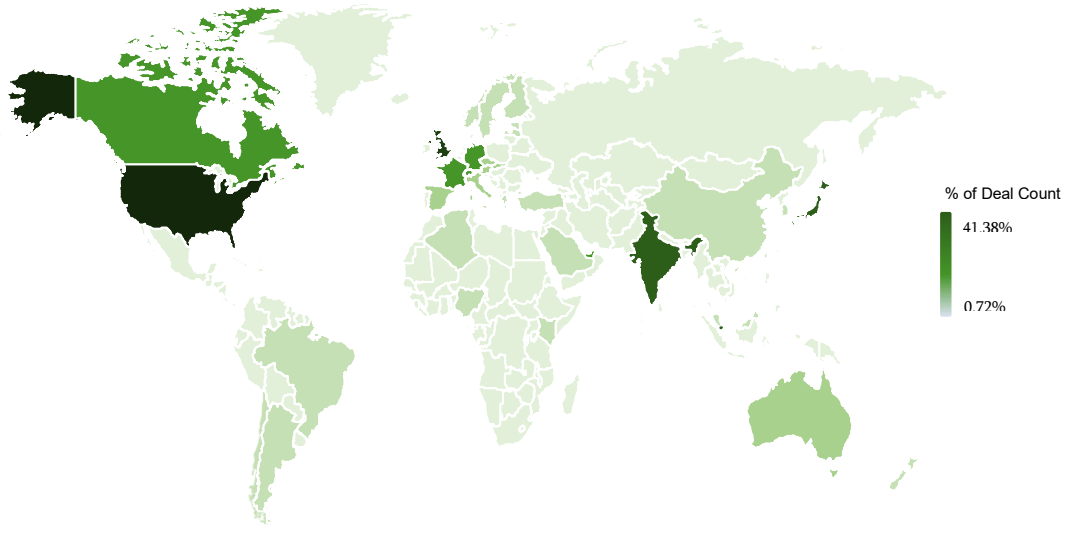

Figure 6. Crypto VC Deals in Q2 2025 by Startup Headquarters Country. Global heatmap showing startup headquarters receiving crypto VC funding in Q2 2025. Source: Galaxy Research.

The United States continues to dominate the crypto startup ecosystem. Despite a remarkably tricky and often (at least, until recently) hostile regulatory regime, companies and projects headquartered in the United States continued to account for most deals completed and most capital invested. The new presidential administration and Congress have begun enacting the most pro-crypto policies in history across a range of vectors. We expect that U.S. dominance will increase, particularly if policies such as implementing regulations for stablecoins and market structure legislation, solidify as expected, which would allow traditional U.S. financial services firms to enter the space in earnest.

4.2.6 Capital Invested by Category

Crypto VC Capital Invested by Category (Q2 2025)

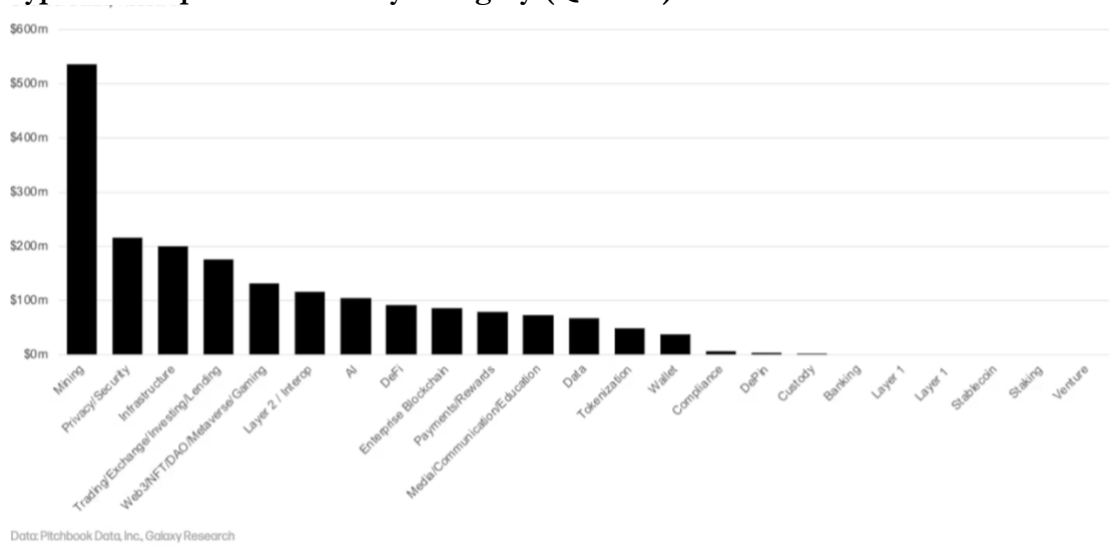

Figure 7. Crypto VC Capital Invested by Category (Q2 2025). Investment by industry category in Q2 2025. Source: Pitchbook Data, Galaxy Research.

In Q2 2025, investment was heavily concentrated in a few categories. Mining led with over $500M raised, followed by privacy/security and infrastructure startups, which each attracted more than $200M. Trading, exchange, and lending platforms also secured meaningful funding, while other verticals such as AI, DeFi, and enterprise blockchain drew smaller but steady allocations. The sectoral skew reflects both immediate catalysts, such as the Bybit security breach fueling demand for improved safety, and longer-term needs for scaling blockchain infrastructure.

Share of Crypto VC Capital Invested by Category (Q2 2025)

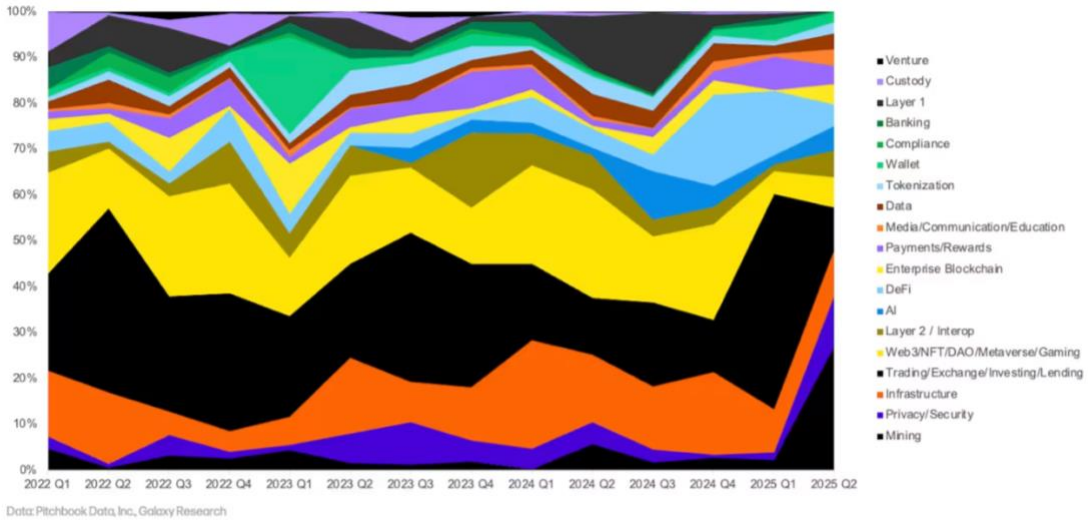

Figure 8. Share of Crypto VC Capital Invested by Category (Q2 2025). The stacked area chart shows the evolution of sectoral allocation from 2022 to 2025 Q2. Source: Pitchbook Data Inc., Galaxy Research.

The relative allocation of crypto VC funding has shifted substantially since 2022. During the ICO- and DeFi-driven peaks of 2021–2022, capital was spread across exchanges, Web3 projects, and infrastructure. By 2025, however, mining, privacy/security, and infrastructure together account for the majority of investment, reflecting a pivot toward core security and scaling solutions rather than speculative token projects. This transition highlights the sector's maturation, with investors prioritizing resilience, compliance readiness, and foundational infrastructure over experimental applications.

4.2.7 Capital Invested by Round Size and Stage

Funding Rounds by Size in Q2 2025

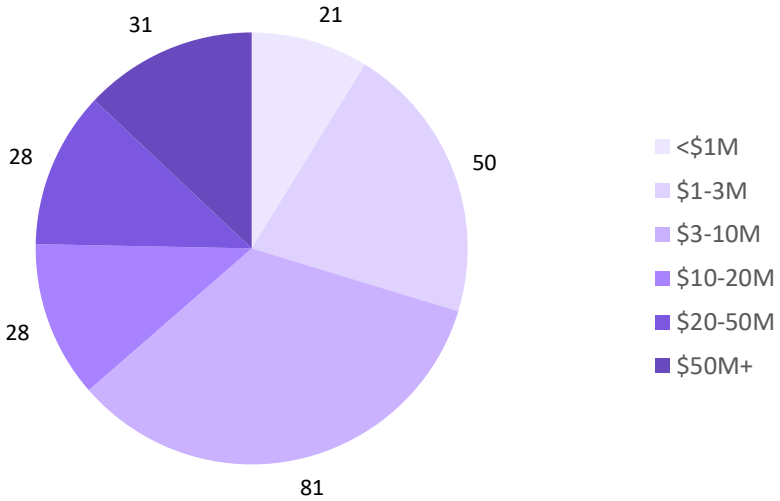

Figure 9. Funding Rounds by Size in Q2 2025. The pie chart illustrates the distribution of funding rounds by size. Source: CryptoRank.

In Q2 2025, most crypto VC rounds were concentrated at the smaller end of the spectrum. Rounds between $1–3M (50 deals) and $3–10M (81 deals) accounted for the majority of activity, highlighting ongoing support for early growth startups. Larger rounds were less frequent, with only 31 deals above

$50M, reflecting investor caution in committing substantial capital despite a few headline raises. The distribution suggests a market still characterized by incremental funding rather than widespread mega-deals, with a reported total of $10.02B.

Funding Rounds by Stage in Q2 2025

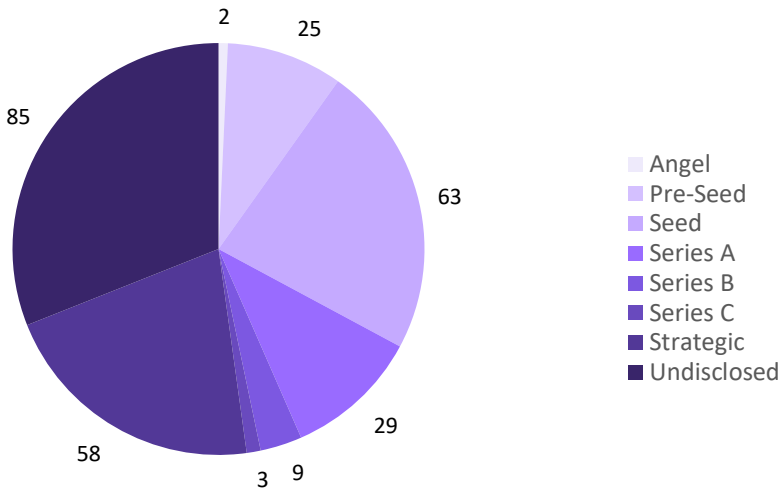

Figure 10. Funding Rounds by Stage in Q2 2025. The pie chart illustrates the distribution funding rounds by stage. Source: CryptoRank.

By stage, Q2 2025 activity was dominated by early phases. Pre-seed (63 deals), seed (29 deals), and Series A (58 deals) made up a large share of the total 274 rounds reported by CryptoRank, confirming investor focus on early development despite recent volatility. Later-stage financing was less common, with just 9 Series B and 3 Series C deals recorded, while strategic rounds (2 deals) played only a marginal role. Interestingly, 85 rounds were undisclosed, displaying persistent opacity in reporting across parts of the crypto ecosystem.

4.2.8 2025: Q1-Q2

Crypto VC funding more than doubled to $6 billion in Q1 2025, led by Binance's $2 billion raise from MGX - the largest crypto minority investment we have tracked. Stablecoins defied the broader crypto market downturn, adding $25 billion in circulation. Our expectation remains that startups monetizing this increasing stablecoin velocity present promising near-term opportunities. Meanwhile, the $1.4 billion Bybit hack could accelerate funding for security and custody solutions. On the exit side, Circle's pending IPO represents the most important price-discovery event for crypto equity since Coinbase listed in 2021.

In Q2 of 2025, venture capitalists invested $1.976 billion (-59% QoQ) into crypto and blockchain-focused startups across 378 deals (-15% QoQ). In Q2 2025, 52% of capital was invested in later-stage companies, while 48% went to earlier stage companies. This is the second time that later-stage investment has exceeded early-stage investment since Q1 2021. The mining category led with a $300 million investment in cloud-mining firm XY Miners, followed by $200m+ invested in the privacy/security and infrastructure categories. The U.S. dominated capital and deal count again, reclaiming the top spot after MGX's Binance investment pushed Malta to No. 1 last quarter. On the fundraising side, investors allocated $1.76 billion to 21 new crypto venture funds.

4.3 What's next?

Looking ahead, crypto venture capital faces a horizon that is less a linear trajectory and more a branching landscape of possibilities. The post-FTX reset and the sharp contraction in Q2 2025 confirm that the sector remains highly sensitive to macroeconomic shifts, regulatory announcements, and idiosyncratic shocks. At the same time, the persistence of deal activity, the partial recovery from the 2023 trough, and the growing share of later-stage and infrastructure-focused rounds suggest that crypto has become a durable, although still contested, part of global venture portfolios. Whether this position strengthens or dissipates will depend on how a number of unresolved questions evolve in parallel across markets, regulatory systems, and governance regimes.

From a capital allocation perspective, the evidence points toward selective rather than indiscriminate deployment. Deal counts have stabilized at levels far below the 2021 to 2022 peak, while capital has concentrated in mining, security, and infrastructure. This pattern fits a regime in which investors back fewer, more defensible projects that satisfy higher standards on technical robustness, governance quality, and regulatory preparedness. It is not clear, however, whether such discipline will persist if macro conditions ease or if a new retail-driven token rally increases asset prices. Will the next phase resemble a more conventional growth-equity cycle, or could renewed speculative appetite once again pull capital toward thinly governed and high-velocity token projects?

Geographically, the contours of the ecosystem are also unsettled. The United States currently dominates both capital and deal count, with the United Kingdom emerging as a secondary hub and Japan and Singapore offering selective depth. Yet the distribution of activity is fragile. How founders and investors arbitrate between these environments is an open question. Will capital concentrate in jurisdictions that offer the clearest rules, or those that offer the greatest flexibility? Will geographic specialization emerge, with some hubs focusing on regulated infrastructure and others acting as centers for DeFi and governance experimentation?

On the regulatory front, the most important transition is from legislative design to interpretive practice. MiCA and the GENIUS Act reduce uncertainty around stablecoins and crypto-asset service providers, but they leave unresolved the more fundamental corporate-law and governance questions highlighted in this report. The legal status of DAOs, the allocation of fiduciary duties in multi-entity arrangements, and the position of token holders who exercise governance rights are all open questions. As supervisory authorities, courts, and private litigants confront concrete disputes about hacks, token allocations, and governance failures, their decisions will effectively create the institutional layer that the legislation does not yet provide. Whether courts continue to rely on doctrines of unincorporated associations and general partnerships, or whether new statutory forms emerge to accommodate decentralized governance, remains uncertain.

The architecture of investment instruments is similarly in flux. Hybrid deals that combine equity, tokens, and governance rights have become increasingly common, but their design remains far from standardized. It is likely that the next cycle will introduce more complex contractual and on-chain arrangements. Token vesting may become linked to governance behavior. Equity rights may be conditioned on protocol-level metrics. Structured products could separate economic rights from voting power in protocol treasuries. Whether these developments strengthen investor-founder alignment or introduce new forms of opacity is an open empirical question. It also remains unclear how limited partners will evaluate portfolios whose liquidity and risk profiles differ significantly from traditional venture capital.

For founders, these uncertainties translate into a more demanding environment. The next cycle is likely to reward teams that integrate technical defensibility, governance design, and legal strategy from the very

beginning, rather than treating compliance and governance as secondary concerns. Still, it is not evident whether this will produce convergence around a small set of standardized organizational templates, or whether ongoing experimentation will preserve a diverse set of structures. Some projects may increasingly internalize institutional investors' expectations, while others may remain deliberately outside formal regulatory perimeters, accepting greater legal and financing risk in exchange for autonomy.

At the ecosystem level, the central question is whether crypto can evolve from a cycle-sensitive narrative asset into an infrastructure-grade component of the financial system. The shift of VC funding toward infrastructure, security, and compliance-related categories is a necessary condition for such a transition, but far from sufficient. Much will depend on broader exogenous factors, including monetary policy, geopolitical tension, and the willingness of financial incumbents to integrate or adopt blockchain infrastructure. Endogenous factors are equally important. The credibility of governance processes, the ability to manage failures, and the fairness of token distribution and exit outcomes will shape whether users and regulators view these systems as trustworthy.

In short, the future of crypto venture capital remains open. It is uncertain whether regulatory convergence or regulatory competition will dominate, whether governance will move toward greater accountability or more sophisticated forms of concentration, and whether hybrid financial instruments will deepen alignment or introduce new conflicts. The answers to these questions will depend not only on technological innovation, but on the evolving interaction among capital, governance, and law. The next phase of crypto VC will therefore not be defined by a single trend but by a series of institutional choices whose outcomes remain very much in flux.

5. Legal and Regulatory Framework

A striking feature of recent regulatory developments, most notably MiCA in the EU and the GENIUS Act in the United States, is that they primarily address financial regulation: token issuance, stablecoin reserves, market abuse, and service-provider licensing. By contrast, the domain in which crypto/web3 ventures most fundamentally diverge from traditional firms (i.e. business and corporate law) remains largely unaddressed. This gap concerns not the classification of tokens as securities or the prudential treatment of stablecoins, but the more foundational legal questions of organizational form, personhood, governance authority, fiduciary duties, and liability. These issues determine how crypto ventures can be formed, controlled, and held accountable, yet existing legal frameworks provide no coherent answers.

Despite the rhetoric of decentralization, many blockchain projects operate through multi-layered institutional architectures that combine (i) a corporate entity developing the protocol, (ii) a foundation or non-profit holding intellectual property and token reserves, and (iii) a DAO coordinating governance through token voting. Corporate law (in both civil-law and common-law jurisdictions) has not been adapted to recognize this structure. As a result, several key governance and liability questions remain unresolved.

5.1 Remaining Gray Areas: DeFi, DAO Liability, Token Classification

5.1.1 Decentralization and Corporate Form

Corporate law traditionally presupposes a legally recognized entity (such as a corporation, LLC, or association) with identifiable managers, clear decision-making authority, and a fiduciary hierarchy. Blockchain-based organizations challenge this paradigm by distributing control across token holders and smart contracts rather than a centralized board.

This creates structural uncertainty in two respects.

First, most legal systems do not recognize DAOs as corporate persons. Outside a few experimental frameworks (e.g., Wyoming's DAO LLC statute and the Marshall Islands' DAO LLC regime), no jurisdiction provides a stable corporate form designed for decentralized governance. Even where DAO LLC forms exist, empirical evidence suggests limited adoption due to incompatibility with token-based participation and cross-border governance.

Second, corporate law lacks a theory of "on-chain decision-making." Token-based voting may be economically meaningful, yet it has unclear legal status. A DAO vote that authorizes treasury spending, changes protocol parameters, or elects delegates does not automatically constitute a legally binding act of the entity responsible for the protocol, unless an off-chain entity explicitly recognizes and operationalizes that decision. This disconnect between on-chain governance and off-chain legal personality is a fundamental structural ambiguity that neither MiCA nor U.S. legislation attempts to resolve.

5.1.2 DAO Liability

The most significant corporate-law risk arises from the question of liability.

Two recent U.S. cases (CFTC v. Ooki DAO and Sarcuni v. bZx DAO) have established an important judicial trend: where no corporate wrapper exists, courts are inclined to treat DAOs as unincorporated associations or even general partnerships.

Under these doctrines:

- participants who vote in governance may be treated as "members,"
- decision-makers may owe duties analogous to partners,
- and members can potentially face joint and several liability for protocol-level actions.

In Ooki DAO, the Northern District of California held that individuals who actively participated in governance by voting their tokens could be treated as members of an unincorporated association. This classification carried two major consequences. First, it provided the Commodity Futures Trading Commission (CFTC) with a legally cognizable defendant: the DAO itself, as a collective entity, was deemed capable of being sued and served. Second, by treating voting token holders as "members," the court effectively attributed the DAO's regulatory violations to the individuals exercising governance power. The court's reasoning rested on traditional principles of association law: when a group of persons acts in concert to pursue a common business purpose (in this case, operating a margin-trading protocol) participation in collective decision-making may suffice to establish membership, even if the group lacks formal incorporation. This approach implicitly rejects the idea that "decentralization" alone shields participants from legal responsibility and instead presumes that functional participation in governance creates legal personality and assignable liability.

In Sarcuni v. bZx, the same jurisdiction extended this logic further by refusing to dismiss claims on the theory that the bZx DAO could plausibly be characterized as a general partnership under California law. The court emphasized that (i) token holders collectively contributed capital (through tokens), (ii) they shared in economic upside (via token appreciation and protocol revenue), and (iii) they exercised joint control through governance proposals. Under default partnership principles, these elements may constitute a partnership formed by conduct rather than contract, leading to joint and several personal liability for wrongful acts committed by the enterprise. Importantly, the court rejected the argument that token-based governance is too diffuse or informal to constitute the requisite mutual agency. Instead, it focused on the economic substance of the arrangement: a group of persons coordinating to run a profit-seeking protocol using pooled resources and shared decision rights.

Taken together, Ooki DAO and bZx signal a judicial willingness to apply default business-association law to decentralized structures whenever no valid corporate wrapper exists. The implications are profound. If courts broadly adopt these interpretations, then any actor who votes tokens (individual users, protocol contributors, delegated voters, or venture investors accumulating governance stakes) may incur personal liability for regulatory breaches, smart-contract failures, or torts attributable to the protocol. Moreover, venture capital funds delegating governance to employees, advisors, or university clubs may inadvertently expose those agents (and possibly the funds themselves) to liability ordinarily avoided through limited-liability entities. The emerging case law therefore challenges a central assumption of DAO design (that decentralization diffuses responsibility) and instead suggests that, in the absence of a recognized legal wrapper, participation in governance may re-centralize liability onto identifiable persons. This legal trend remains embryonic but constitutes the most significant corporate-law risk currently facing DAO-based governance systems.

European private law does not yet provide equivalent case law, but the underlying problem is the same: absent a recognized legal wrapper, DAO participants risk falling into default categories of entity law that assign unlimited liability. MiCA does not create a corporate form for DAOs; nor does it harmonize Member State private law on the matter. As ESMA itself notes in its MiCA workstreams, the treatment of DAOs "requires further assessment within general private-law frameworks," a phrasing that implicitly acknowledges reliance on existing corporate-law categories rather than the creation of new ones.

5.1.3 Token Classification

Whereas securities regulation focuses on whether a token is a financial instrument, corporate law asks a different question: what legal relationship exists between the token holder and the entity (or entities) behind the protocol?

For most projects, the answer is: none that is clearly defined.
Tokens may carry governance rights, access rights, or even economic rights, but corporate law does not recognize token holders as shareholders, beneficiaries, creditors, or members of an entity unless a specific corporate structure creates such a relationship.

This gap produces several consequences:

1. Governance rights without fiduciary protection
Token holders who can influence protocol decisions typically receive no fiduciary duties from founders, contributors, or foundation council members.

2. Treasury claims without enforceability
Token holders may have expectations about the use of treasury funds or revenue-sharing mechanisms, yet these mechanisms rarely create enforceable claims in corporate law.

3. Cross-entity ambiguity
Many protocols operate through one entity (foundation), while development is conducted by another (OpCo), and tokens are governed by a third (DAO). There is no established doctrine to determine which entity owes obligations arising from token governance.

4. Classification spillovers
Even if a token escapes securities regulation (as under the GENIUS Act for certain stablecoins or under MiCA for certain utility tokens), its corporate-law status remains unresolved, leaving holders in a legally indeterminate position.

As a result, token holders often occupy a structurally novel position: economically exposed to the performance of a protocol, capable of influencing governance outcomes, yet not linked to any legally recognized corporate relationship. This "governance without legal personality" represents one of the most significant corporate-law challenges of the Web3 ecosystem.

6. How do Venture Capitalist Invest?

6.1. Equity-Only Investments

In the blockchain and crypto ecosystem, not all venture capital transactions involve tokens. A significant subset of early-stage and growth capital continues to be deployed through traditional equity-only deals, especially when the investee is a company building products, infrastructure, or services around crypto protocols but not directly issuing a native token. This includes firms in custody, analytics, security, developer tooling, and financial infrastructure.
Equity-only investments provide venture capitalists with contractual rights under corporate law - rather than cryptographic governance rights via tokens. These transactions typically involve convertible notes**,** SAFEs (Simple Agreements for Future Equity)**,** or preferred stock, depending on the stage and structure of the startup.

6.1.1. Convertible Notes

Convertible notes are debt instruments that convert into equity during a future priced round, usually at a discounted valuation or subject to a valuation cap. In crypto startups, they are commonly used at the pre-seed or seed stage, when founders want to raise capital quickly while delaying the formal valuation process.

Key features:

- Maturity and interest: Convertible notes accrue interest and have a maturity date, after which they must either convert or be repaid—though repayment is rare in practice.
- Discount and cap: Early investors typically receive either a discount (e.g., 20%) on the next round valuation or benefit from a valuation cap that sets a maximum conversion price.

In crypto, convertible notes can be used for companies with unclear token roadmaps or in regulated jurisdictions where token sales are legally risky. However, when token issuance is a future possibility, notes often include side letters or separate agreements to ensure investors receive proportional token allocations once tokens are live. These informal arrangements, sometimes structured as token warrants or non-binding letters of intent, create legal ambiguity and may not always be enforceable.

6.1.2. SAFEs (Simple Agreements for Future Equity)

SAFEs are an alternative to convertible notes designed to be more founder-friendly. Originally developed by Y Combinator, SAFEs are not debt instruments: they carry no interest, no maturity date, and are simpler to administer.
Key features:

- Trigger event: SAFEs convert into equity upon the next priced equity financing.
- Valuation cap/discount: Like notes, SAFEs offer early investors favorable conversion terms via a cap and/or discount.
- No repayment obligation: If the company fails or never raises, the SAFE expires worthless.

In crypto, SAFEs are widely used at the pre-token stage. In purely equity-only deals, the SAFE may grant no rights to future tokens. However, many SAFEs now include "side letters" or token side agreements, especially if the founders anticipate launching a protocol and distributing a governance token later. These

hybrid or contingent rights can blur the line between equity-only and token-linked financing, depending on how they are disclosed and enforced.
In some jurisdictions, modified SAFEs that explicitly mention tokens may come under regulatory scrutiny, especially if they resemble investment contracts under securities law.

6.1.3. Preferred Stock

Preferred equity becomes the dominant instrument at the Series A stage and beyond. In crypto companies that avoid tokenization or whose tokens are governed separately by a DAO, preferred stock remains the most robust way for VCs to obtain governance rights, board access, and economic protection.
Key features:

- Board and voting rights: Investors often gain board seats, information rights, and protective vetoes on major decisions.
- Liquidation preferences: Ensures capital return before common shareholders in case of sale or liquidation.
- Anti-dilution protection: Shields early investors if new shares are issued at a lower valuation.
- Participation rights: Gives investors the option to join future financing rounds to maintain ownership.

Examples of crypto companies that have raised through equity-only preferred stock rounds include:

- Fireblocks (custody infrastructure)
- Ledger (hardware wallets)
- Chainalysis (blockchain analytics)
- Blockdaemon (staking infrastructure)

These firms have built critical services within the crypto economy while maintaining a traditional corporate governance model. In many cases, there is no native token, and even where one exists at the protocol level, it is legally and functionally decoupled from the operating company.

6.1.4. Notable Examples of Equity-Only Investments

Several well-capitalized crypto infrastructure companies have built and scaled without issuing native tokens or relying on protocol governance. Instead, they operate as traditional corporations, with value accruing to equity holders through established legal frameworks. These firms provide essential services (custody, analytics, developer tooling) across the blockchain ecosystem, while remaining outside of the token-based governance paradigm.

Fireblocks
Fireblocks is a provider of institutional-grade custody and digital asset infrastructure. Since its founding, it has raised over $1.2 billion in equity funding, reaching a valuation of $8 billion as of 2022. Its offering (wallet technology, transfer networks, and MPC-based security) targets financial institutions and exchanges. Investors include Sequoia, Coatue, and Ribbit Capital. Fireblocks does not operate a protocol, does not issue a native token, and remains governed through a conventional corporate structure.

Ledger
Ledger manufactures secure hardware wallets (Nano S, Nano X) used by retail and institutional users to store cryptocurrencies. In 2021, it closed a $380 million Series C round at a $1.5 billion valuation, led by 10T Holdings. Ledger has never launched a token nor externalized governance to a DAO. Its business

model is based on product sales, brand security, and user trust, making equity the central investment instrument for participating VCs.

Chainalysis
Chainalysis offers blockchain forensics, compliance, and transaction monitoring solutions, primarily to regulators, law enforcement, and crypto exchanges. It has raised over $500 million through equity financing, with support from Accel, Paradigm, and Benchmark. Chainalysis operates entirely as a centralized data analytics firm, without a protocol layer, without a governance token, and without plans for decentralization.

Blockdaemon
Blockdaemon builds staking infrastructure and institutional node services. In 2021, it raised $155 million in a Series B round that brought its valuation to over $1.2 billion. Investors include SoftBank, Kraken Ventures, and Goldman Sachs. Despite operating deep within decentralized networks, Blockdaemon itself does not issue a token nor engage in DAO governance. The company's revenues are service-based, and investor participation is structured entirely via equity.

6.2. Token-Only Investments

Venture capital investment in the blockchain ecosystem increasingly includes *token-only transactions*, in which VCs acquire native or governance tokens rather than traditional equity. Unlike startup shares, which represent legal ownership and corporate control, tokens can carry a wide range of functions - from governance rights in a decentralized protocol to access privileges, yield accrual, or economic exposure to the network's success. Token-only deals offer faster liquidity, flexible structuring, and native alignment with decentralized ecosystems - but also raise complex legal, financial, and custodial considerations.

This section examines the key instruments, legal structures, custody frameworks, and liquidity mechanisms underlying token-only VC investments, with a particular focus on SAFTs (Simple Agreements for Future Tokens), direct token purchases, and the mechanisms of vesting and token unlock schedules.

6.2.1. SAFTs: A Structured Entry into Tokens

The Simple Agreement for Future Tokens (SAFT) emerged as the standard legal framework for token-only investments, especially in early-stage blockchain projects. Inspired by the SAFE (Simple Agreement for Future Equity) used in startup financing, the SAFT allows investors to provide capital upfront in exchange for the right to receive tokens at a later date, typically once the network is operational and the token is publicly launched.

The typical SAFT is a private contract between the issuer (i.e., the startup) and the investor (VC fund or crypto-native firm), which outlines:

- Purchase price (often discounted relative to public sale or fair value)
- Token allocation
- Vesting schedule and delivery mechanics
- Trigger conditions (e.g., launch, protocol upgrade, regulatory approval)

SAFTs are especially common in jurisdictions like the U.S., where pre-functional tokens are still considered investment contracts under the Howey Test and thus subject to securities regulation. By deferring token delivery and restricting transferability, the SAFT model aims to delay the moment at which the token could be considered a public offering.

However, SAFTs have drawn criticism on two fronts. First, they blur the line between equity and utility by offering tokens that may eventually function as securities, governance tools, or access mechanisms. Second, the SAFT presumes that tokens are not securities at launch, a legal gray area in many jurisdictions.

In practice, many VCs structure token deals via SAFTs to gain early access at discounted valuations, and the tokens received under SAFTs are often subject to lock-up periods or delayed issuance, depending on the project's stage and risk profile.

6.2.2. Direct Token Purchases: Strategic and Liquid

Some VC funds engage in direct token purchases, especially when investing in projects that have already launched a live token with active market trading. These deals often occur via:

- Treasury sales: where the protocol sells tokens directly to the investor
- OTC (over-the-counter) deals: peer-to-peer negotiations for large blocks
- Governance proposals: in which the DAO votes to allocate treasury tokens to strategic backers

Direct purchases give investors immediate access to governance and liquidity. In the case of live governance tokens (e.g., UNI, AAVE, MKR), direct buyers can start participating in governance votes, forum discussions, and even protocol treasuries. In many cases, VC firms coordinate token purchases with governance engagement, either by acquiring voting power directly or delegating votes to friendly third parties (e.g., university blockchain clubs or public goods DAOs).

However, direct token deals raise concerns about:

- Market impact: Large purchases can affect price volatility or signal insider trading.
- Reputational risk: Sudden token sales ("VC dumps") can harm community trust.
- Regulatory ambiguity: If tokens carry voting or revenue rights, they may still be considered securities depending on jurisdiction.

Notably, these deals rarely include legal control rights, and are instead governed by smart contract logic and community enforcement mechanisms. As a result, the relationship between VC and protocol is far more fluid than in traditional equity-based board governance.

6.2.3. Custody, Vesting, and Unlock Mechanics

Token-only investments require specialized mechanisms for custody, vesting, and liquidity control, especially to align incentives, avoid sell-offs, and maintain price stability. Three critical components define post-investment token management:

a. Custody

Unlike shares, which are held by custodians or recorded in cap tables, tokens are bearer assets - whoever holds the private key controls the asset. Institutional investors rely on qualified custodians such as Anchorage, Fireblocks, BitGo, or Coinbase Custody to securely manage token allocations. Custody arrangements may also be integrated with multi-signature wallets, smart contract vaults, or hardware devices depending on the level of decentralization and risk tolerance.

Custody becomes particularly complex when tokens are non-transferrable, subject to vesting, or linked to governance rights that require active participation. In these cases, custody must support not only storage, but staking, delegation, and on-chain voting - features that many traditional financial custodians still lack.

b. Vesting

Token vesting mimics the function of equity vesting in startups: it ensures that capital providers and team members are aligned over time and cannot exit prematurely. Typical vesting schedules in token deals include:

- 12-month cliff + 36-month linear vesting (common for team and advisors)
- 6-month cliff + 18-month linear vesting (VC or early backers)
- Custom schedules tied to network milestones, TVL thresholds, or product launches

Vesting is often enforced via smart contracts, which gradually release tokens to investor-controlled wallets on predefined dates. In some protocols (e.g., Cosmos or Synthetix), vesting contracts are transparent and auditable on-chain, which promotes accountability. However, in less formalized ecosystems, vesting may be off-chain or easily bypassed, leading to concerns about rug pulls or unaligned early backers.

c. Liquidity and Unlock Events

Tokens become liquid when they are:

- Unlocked after vesting
- Listed on centralized or decentralized exchanges
- Transferrable across wallets and bridges

From a VC perspective, token liquidity offers early exit opportunities, often much faster than traditional equity exits (IPO or acquisition). This feature makes token-only investments attractive for funds with shorter time horizons or for managing internal fund liquidity.

However, large unlock events also pose market risks: price crashes, whale sell-offs, and community backlash. Some protocols mitigate this by implementing:

- Staggered unlock schedules
- Cliff extensions based on market conditions
- Re-staking incentives to reduce sell pressure

Protocols may also require investors to commit to governance, ecosystem development, or liquidity provision (e.g., market making or staking) during the vesting period to preserve ecosystem value.

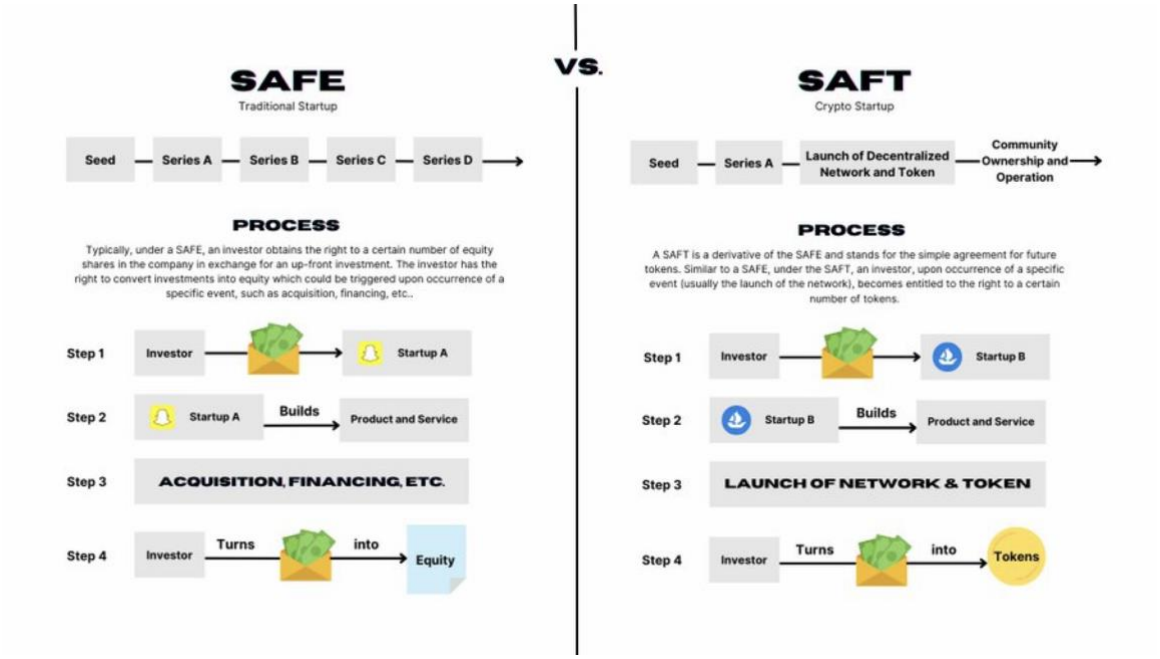

Figure 11. Comparison of SAFE vs. SAFT Financiang Structures. The diagram contrasts startup SAFE (equity conversion) with crypto SAFT (token delivery post-launch).

While traditional startup financing depends on SAFEs that turn into equity, crypto businesses use SAFTs that turn into tokens at network launch. This comparison demonstrates how well-known venture tools are modified for token-based models in crypto financing.

6.3. Hybrid Structures (Equity + Tokens)

As blockchain ventures evolve into complex, multi-layered ecosystems, hybrid investment structures - which combine traditional equity shares with native tokens - have become increasingly common in venture capital deals. These arrangements allow investors to participate both in the corporate upside (via equity ownership) and the network value creation (via tokens), bridging the institutional familiarity of equity with the novel, decentralized mechanisms of crypto-native assets.

This section explores the design, rationale, and challenges of equity-plus-token deals, highlighting how hybrid structures address (or complicate) issues of control, incentive alignment, and legal enforceability.

6.3.1. The Architecture of Hybrid Deals

Hybrid deals involve two distinct instruments:

- Equity shares in a legal entity (typically a C-corp, LLC, or foundation-owned operating company), granting rights to profits, governance, and a share in a potential exit (e.g., IPO or acquisition)
- Tokens issued by the protocol or network governed by that entity (e.g., governance tokens, utility tokens, or staking assets)

VCs participating in these deals typically negotiate dual allocations: a stake in the company *and* a share of the protocol's future token supply. The equity portion aligns with traditional expectations (ownership, control rights, potential acquisition), while the token portion offers a path to network participation, staking yield, liquidity, and in many cases, governance influence.

The most common hybrid deal terms include:

- SAFT + equity warrant: Investor signs a SAFT for tokens, and also receives a warrant to purchase equity.
- Equity round + token side letter: Investor participates in a priced equity round and negotiates a parallel token allocation agreement.
- Simple token warrant: Investor receives a legal agreement entitling them to tokens upon launch, typically linked to equity participation.

These structures are increasingly negotiated by crypto-native law firms (e.g., Latham & Watkins, Cooley, Fenwick & West) that specialize in aligning off-chain ownership with on-chain economics.

6.3.2. Why Hybrid?

Hybrid deals solve a fundamental challenge in Web3 venture building: the protocol and the company are not always the same entity.

Most blockchain ecosystems are built by centralized founding teams that eventually intend to decentralize governance. The legal entity raises funding, hires engineers, and builds the product. The protocol or DAO issues a token to incentivize usage, reward contributors, and secure the network. If the token alone were funded, investors would have no claim on the intellectual property, no recourse in case of failure, and often no control over strategy. If only equity were funded, investors would have no participation in token economics, governance, or liquidity upside.

Hybrid deals therefore reflect:

- Two value layers: the value of the company (IP, codebase, team), and the value of the network (tokens, users, protocol adoption)
- Two incentive channels: investor return through equity exit (e.g., acquisition), and token appreciation or staking yield
- Two control frameworks: corporate governance (board, voting rights) and on-chain governance (token voting, DAO proposals)

Done well, hybrid deals allow VCs to capture value across both dimensions, while also participating responsibly in network governance.

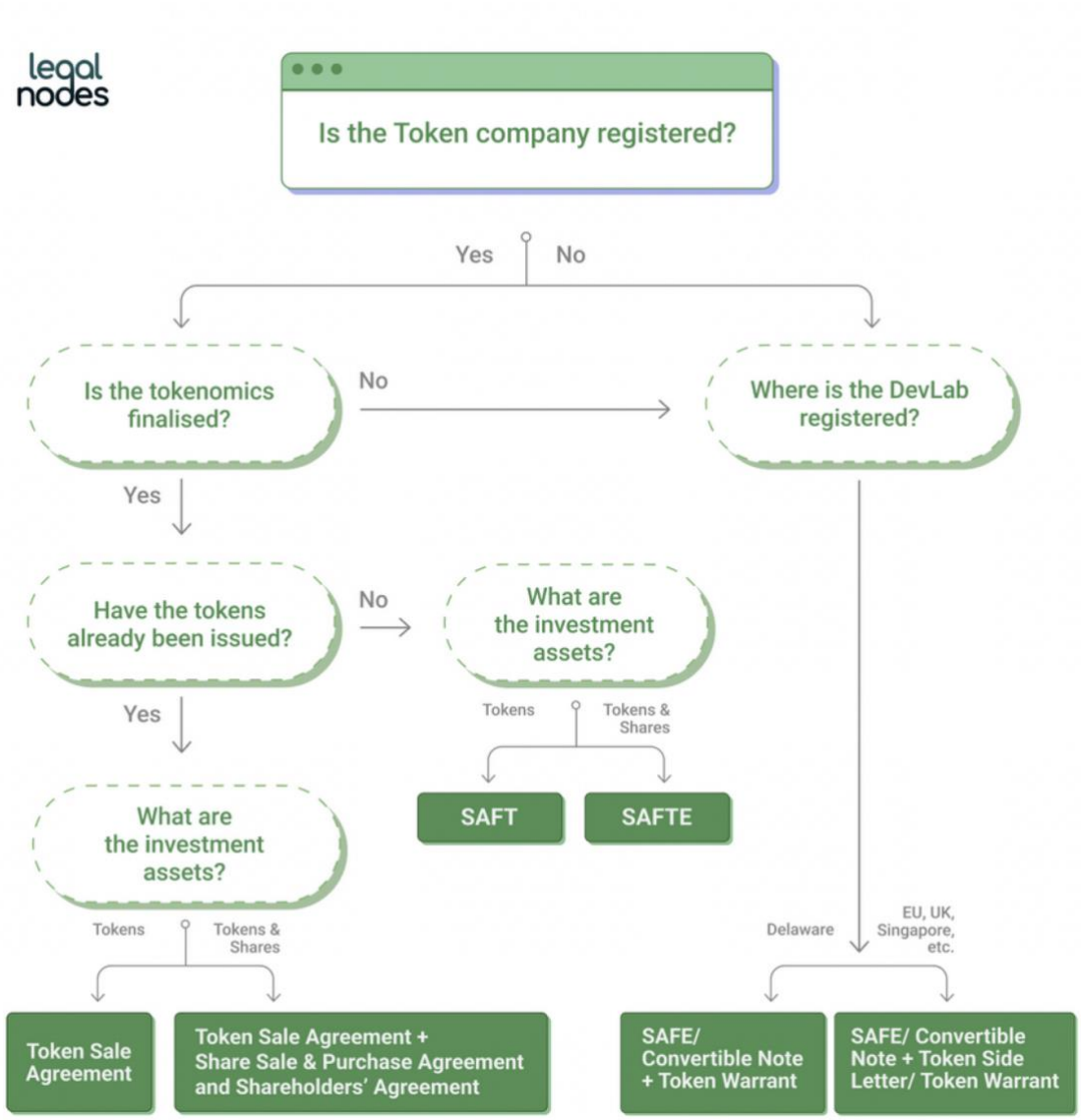

Figure 12. Legal Structure of Hybrid Token Investments. Flowchart showing legal decision paths depending on token registration, jurisdiction and asset type. Source: Legal Nodes.

Depending on the company's registration, tokenomics state of readiness, and whether the assets are shares, tokens, or both, different token investment models apply. This framework demonstrates the application of legal tools like token warrants, SAFT, and SAFTE.

6.3.3. Legal Complexity

Hybrid investment structures - combining equity and token rights - face significant legal complexity. These deals must reconcile the requirements of traditional corporate law with the evolving legal treatment of crypto assets, often across multiple jurisdictions. Five key areas of legal friction emerge:

Securities Classification

In jurisdictions like the U.S., both equity and tokens may be classified as securities, especially when tokens are pre-functional, tied to a central development team, or sold alongside investor protections. This triggers the need for:

- Disclosure and compliance under securities laws

- Restricted transferability
- Investor acknowledgments of risk and limitations

Many hybrid deals include SAFT-like disclaimers, structured vesting, and private placements to navigate these constraints.

Token Allocation Vehicles

Tokens are rarely issued directly by the company receiving equity investment. Instead, rights are typically allocated via:

- Foundations
- Token warrants
- Side letters or token purchase agreements

These multi-entity structures separate the operating company (OpCo) from the protocol treasury, raising enforceability issues. Investors must ensure their token entitlement is legally binding - even if the token-issuing entity is governed by a DAO or offshore foundation.

Jurisdictional Arbitrage

Most hybrid deals involve cross-jurisdictional structuring. For example, the OpCo may be based in the U.S. or EU, while the foundation managing the token treasury is incorporated in Cayman, Switzerland, BVI, or Singapore. This creates friction in:

- Tax treatment of tokens vs. shares
- Disclosure requirements
- Enforcement and transfer rules

Legal teams must bridge these regimes while preserving the economic logic of the hybrid investment.

Token Vesting and Cliff Conditions

Tokens are often subject to vesting schedules, designed to mimic startup equity vesting:

- A common structure includes a 6-month cliff, followed by 24–36 months of linear vesting
- Vesting may be enforced through smart contracts, or managed via DAO votes

However, equity and token vesting often proceed on separate timelines, which can lead to misaligned investor expectations, especially if token liquidity arises before equity exit.

Board Rights vs. DAO Governance

In equity deals, VCs may receive board seats, observer rights, or protective provisions (e.g., veto rights over major decisions). In protocol governance, their influence derives from:

- Token holdings
- Delegation
- Proposal creation and voting behavior

Tensions can emerge when DAO decisions move faster or in different directions than the board, especially in areas like treasury deployment, protocol upgrades, or ecosystem partnerships. In extreme cases, this creates a dual power structure that confuses accountability and strategic focus.

6.3.4. Incentive Alignment (and Misalignment)

Hybrid investments aim to align stakeholders - investors, founders, contributors, and communities - by combining equity-based upside with token-driven network value. In practice, however, these structures often expose misaligned timelines, liquidity windows, and governance incentives.

Token Liquidity vs. Equity Illiquidity

One of the most disruptive elements in hybrid deals is the temporal mismatch between:

- Tokens, which may become tradeable within months after launch
- Equity, which remains illiquid until a private exit or IPO

This creates an incentive for early investors to exit tokens quickly, undermining long-term engagement. Founders and contributors may also prioritize short-term token appreciation over sustainable company growth.

Control (Equity) vs. Participation (Token)

Equity investors exert formal control through legal governance mechanisms - such as board votes or protective covenants. Token governance, in contrast, offers influence without control. VCs may use:

- Delegation to friendly actors
- Participation in proposal discussions
- Voting coalitions or alliances

This asymmetry can result in conflicting behaviors: a VC might oppose a protocol initiative via token governance while supporting a related equity-side decision - confusing stakeholders and diluting strategic cohesion.

Founder Incentives and Dual Wealth Tracks

Founders often receive significant token allocations in addition to equity. If token values increase early, founders may achieve substantial personal wealth long before the equity investors exit. This misalignment can reduce the founder's motivation to pursue a company exit or sustained operational discipline - especially if equity dilution increases over time.

Reputation and DAO Trust

Token communities may view hybrid investors with skepticism, especially when governance participation appears self-serving (e.g., proposals to boost token value or unlock vesting prematurely). In response, some VCs adopt "responsible governance" practices, such as:

- Publishing voting rationales
- Abstaining from conflicted votes
- Participating in governance forums and workshops

- Funding open-source tools or public goods

This effort to build social legitimacy is critical. In tokenized ecosystems, reputation is often as valuable as formal rights, especially when governance is open and adversarial.

6.3.5. Examples of Hybrid Deals

A growing number of high-profile Web3 protocols have adopted hybrid financing structures, issuing both equity and tokens to their early backers. These deals give venture investors parallel exposure to a company's corporate upside and its decentralized protocol economy, typically mediated through a mix of SAFEs, token warrants, direct token allocations, and participation in DAO governance.

While such models promise alignment between traditional capital markets and Web3 ecosystems, they also introduce complex risks. The following examples illustrate how hybrid structures are deployed in practice - and what they reveal about the interaction between legal contracts, incentive design, and decentralized governance.

dYdX: From Centralized Exchange to Tokenized DAO

- Structure: dYdX Labs raised equity funding from leading VCs (e.g., Paradigm, a16z) while separately launching the DYDX governance token.
- Transition: Initially, the protocol operated under centralized control. Over time, the team transferred key protocol functions - such as trading incentives, liquidity mining, and protocol upgrades - to a token-based DAO.
- Token Mechanics: Investors received DYDX tokens subject to vesting and lockups, alongside their equity stake.
- Outcome: dYdX has since announced its transition to a fully decentralized order book (v4) and governance model, governed by token holders rather than dYdX Labs.

Lesson: This staged approach allowed the protocol to scale under centralized control while gradually decentralizing governance. The dual exposure (equity + token) helped VCs remain aligned during the transition, though community concerns have emerged around early token allocations and governance participation by insiders.

Uniswap Labs: Corporate R&D, DAO Governance

- Structure: Uniswap Labs raised traditional equity funding (from a16z, Paradigm, Union Square Ventures, etc.), while the UNI token governs the protocol through a decentralized DAO.
- Token and Treasury: UNI token holders control a multi-billion dollar treasury and protocol-level decisions. Uniswap Labs, the company, retains ownership of the front-end, legal IP, and branding.
- VC Exposure: Leading investors hold both equity in Uniswap Labs and large quantities of UNI, often via direct allocation or secondary market accumulation.

Tension Point: In 2023, controversy erupted when a16z voted against a proposal to deploy Uniswap on BNB Chain, favoring LayerZero (a portfolio company) over Wormhole as a bridge provider. Although legal ownership resided with the Labs, the protocol's DAO governance surfaced a clear conflict between portfolio interests and protocol neutrality.

Lesson: Uniswap exemplifies how dual-track governance can lead to blurred lines of accountability. While hybrid exposure allows for deep involvement, it also creates reputational risk if VCs appear to exert undue influence over supposedly decentralized processes.

Axie Infinity (Sky Mavis): Dual Incentives and Community Trust

- Structure: Sky Mavis, the studio behind Axie Infinity, raised equity funding from firms like a16z, Accel, and Paradigm. Simultaneously, the protocol launched the AXS governance token (and in-game token SLP).
- Token Allocation: Early investors were granted AXS tokens in addition to equity, with vesting schedules designed to align long-term incentives.
- Governance Role: Although nominally governed by token holders, much of Axie's roadmap remained under centralized company control during its growth phase.

Challenge: When Axie's economic model faltered during the 2022–23 bear market, criticism emerged regarding early token sell-offs, VC participation in governance, and whether value was extracted from the community too quickly.

Lesson: Hybrid deals in game-based ecosystems require careful pacing of token unlocks and transparency around governance rights. When community trust is compromised, dual exposure becomes a liability - fueling narratives of extraction and short-termism.

Arbitrum (Offchain Labs): Airdrops, Equity, and DAO Power

Structure: Offchain Labs raised equity from Lightspeed, Polychain, and others, while the ARB token was distributed via an airdrop and is governed by the Arbitrum DAO.

- Token-Ecosystem Link: ARB tokens were granted not just to users but also to early investors and contributors, often via DAO treasury allocations or foundation reserves.
- Governance Crisis: In 2023, the Foundation allocated nearly $1 billion in tokens to itself before DAO approval, leading to a backlash and rejection vote from the community. While not all investors were directly involved, the governance optics cast doubt on whether the token-holder community could restrain top-down decisions.

Lesson: Hybrid structures must be supported by clear governance sequencing. When token governance appears symbolic or post hoc, it undermines the legitimacy of decentralization - even when equity-backed investors remain passive.

Flexibility and Fragility in Hybrid Deals

These case studies highlight a shared pattern: hybrid structures offer protocols the flexibility to raise venture capital while building open, decentralized ecosystems - but that same flexibility can lead to fragility if stakeholders are not clearly aligned.

When structured well:

- Hybrid deals bridge traditional legal systems and decentralized innovation, supporting capital formation, community participation, and long-term development.
- VCs can support protocol growth via technical support, liquidity provisioning, and responsible governance participation.

- Dual exposure fosters continuity across the protocol's lifecycle - from early R&D to decentralized governance.

When structured poorly:

- Misaligned incentives (e.g., token liquidity before equity exit) may lead to early exits, governance apathy, or conflicting strategies.
- Legal ambiguity and unclear role boundaries can produce conflicts between the company and the DAO.
- Community backlash may emerge if governance is seen as opaque, captured, or extractive.

6.4 Governance Token Acquisitions

DAO Voting, Treasury Access, Protocol Control, and Delegation Strategies

As decentralized protocols mature, governance tokens have become a key entry point for venture capitalists (VCs) seeking to influence and participate in blockchain ecosystems. Unlike traditional equity, governance tokens typically do not confer legal ownership, but instead grant holders the ability to participate in protocol decision-making - such as proposing upgrades, allocating treasury funds, adjusting economic parameters, or voting on key strategic directions.

In recent years, governance token acquisitions have emerged as both a strategic investment vehicle and a tool for protocol capture or alignment - depending on how they are structured and exercised. This section explores the nature of governance tokens, the dynamics of DAO (Decentralized Autonomous Organization) voting, the use of delegation and soft power by VCs, and the risks and opportunities involved in investing via governance rights rather than equity ownership.

6.4.1. What Are Governance Tokens?

Governance tokens are crypto-native assets that give holders the ability to influence or control the operations of a decentralized protocol, typically through on-chain or off-chain governance mechanisms. Most DAOs are governed by such tokens - examples include UNI (Uniswap), COMP (Compound), AAVE (Aave), and MKR (MakerDAO).

Typical governance token rights include:

- Voting on protocol upgrades (smart contract changes, new product launches)
- Allocating or approving treasury funds (grants, liquidity mining, contributors)
- Modifying fee structures, staking rewards, inflation parameters
- Approving cross-chain deployments or partnerships
- Electing or replacing DAO working groups or multisig signers

Importantly, governance tokens are often transferrable, divisible, and liquid - meaning that influence in the protocol can be bought, sold, and accumulated in secondary markets. This opens the door to strategic accumulation of governance power by large token holders, including VCs, whales, and ecosystem players.

6.4.2. How VCs Acquire Governance Tokens

There are three main paths through which VCs acquire governance tokens:

a. Early Allocation via Token Sales

VCs often acquire governance tokens during:

- Pre-seed or seed rounds via SAFTs or token purchase agreements
- Treasury sales approved by the DAO itself
- Ecosystem grants or allocations (sometimes non-dilutive)

These deals typically include vesting schedules to avoid immediate sell pressure and to signal long-term commitment. For example, Paradigm, a16z, and Polychain received early allocations of tokens like UNI, DYDX, and MKR under multi-year vesting.

b. Secondary Market Accumulation

Once a token is liquid, investors may purchase governance tokens on the open market, either directly or via OTC (over-the-counter) deals. This approach allows for flexible entry, but also raises concerns about "governance sniping" - where investors acquire influence rapidly without prior involvement.

Examples include activist whales accumulating tokens right before high-stakes votes, sometimes to sway decisions or force treasury actions.

c. DAO-led Treasury Sales or Partnerships

Protocols may vote to sell governance tokens to strategic partners in exchange for funding, liquidity, or support. These sales are on-chain, transparent, and require DAO approval, often through governance proposals.

While ostensibly decentralized, such sales may be pre-negotiated off-chain with investors before public votes, raising questions about the true independence of the DAO.

6.4.3. What VCs Do with Governance Tokens

Holding governance tokens gives venture capital investors a unique form of non-corporate influence, often comparable to board-level power in traditional firms - yet exercised without fiduciary obligations or formal responsibilities. This influence plays out in three main domains: voting, treasury access, and protocol parameter control.

Voting on Proposals

Active participation in governance forums and on-chain proposal voting allows VCs to help shape the strategic direction of a protocol. For instance, a16z famously voted against Uniswap's proposal to deploy on BNB Chain, citing security concerns - though critics pointed out that a16z's preferred bridge provider, LayerZero, was a portfolio company. In other protocols, major VCs such as Polychain regularly participate in votes that determine treasury disbursements, the creation of ecosystem funds, or even the restructuring of DAO governance itself.

Access to DAO Treasuries

Governance tokens often confer indirect access to multi-million dollar DAO treasuries, enabling holders to:

- Propose or approve grants for research, tooling, or integrations
- Fund working groups or "core units" that handle legal, technical, or marketing functions
- Co-author proposals with contributors to steer capital toward sectors aligned with their broader investment theses

In some cases, VCs set up or support dedicated working groups within a DAO - either publicly or behind the scenes - to ensure alignment with their interests.

Control over Protocol Parameters

In more sophisticated protocols like MakerDAO, governance token holders directly vote on key system parameters, including:

- Stability fees and borrowing costs
- Collateral asset onboarding
- Risk tolerance thresholds
- Oracle infrastructure and incentives

This type of governance can have monetary policy implications. Large token holders effectively act as macro-level stewards, shaping the internal economy of the protocol with consequences for users, borrowers, and integrated DeFi systems. In this sense, a VC with concentrated token holdings may operate like a central bank or regulatory board, without the institutional checks that normally accompany such roles.

6.4.4. Delegation Strategies and the Use of Soft Power

To avoid the reputational and regulatory risks of overt governance control, many VCs delegate their voting power to third parties. These include technical contributors, public goods advocates, university blockchain clubs, or respected DAO members.

This strategy serves multiple purposes:

- It masks direct control while retaining influence
- It legitimizes governance through the voice of credible community delegates
- It complies with jurisdictional concerns around active protocol management

A well-known example is a16z's delegation of large UNI stakes to the Harvard, Stanford, and Michigan blockchain clubs. While the votes were cast by the clubs, the underlying alignment with a16z's strategic preferences was widely observed. This "soft power" dynamic is a hallmark of mature DAO politics: formal decentralization coupled with informal coordination.

Delegation itself is executed via governance tools like Tally, Snapshot, or Agora, which allow token holders to assign their voting rights without transferring ownership. Delegation is publicly visible and revocable, making it both transparent and contestable. In many DAOs, delegates now campaign for support, publish voting reports, and build reputations as reliable stewards - effectively becoming protocol politicians.

VCs also exercise soft power beyond formal delegation. This includes:

- Influencing forum discussions and setting narrative agendas
- Funding governance tooling, research, or proposal drafting
- Coordinating informally with aligned DAOs or delegates to build voting coalitions

In practice, these forms of networked influence often resemble traditional political lobbying or shareholder activism, where authority emerges not from legal title, but from access, narrative framing, and off-chain coordination.

6.4.5. Governance Capture vs Legitimate Participation

The distinction between governance capture and strategic engagement is often blurry. A venture investor who helps launch and fund a protocol arguably has a legitimate interest in shaping its direction. However, concerns arise when:

- Token allocations are heavily concentrated among insiders
- Delegation structures obscure real control
- Proposals disproportionately benefit affiliated projects or companies

The Uniswap–LayerZero incident is illustrative: although the vote was framed as a technical choice between bridge providers, it exposed the deeper tension between protocol neutrality and portfolio alignment. In Arbitrum, controversy erupted when the Foundation transferred millions of tokens to itself prior to a governance vote, raising concerns about procedural legitimacy - despite VCs not being directly implicated.

In response to these concerns, some investors are adopting a "responsible governance" approach. This includes:

- Publishing voting rationales
- Abstaining from votes where conflicts of interest exist
- Funding neutral ecosystem grants
- Participating in open governance workshops and policy design forums

Protocols like Optimism have gone a step further, assigning governance powers to non-financial actors, such as the Citizens' House in their retroactive public goods funding model. These experiments aim to decouple economic weight from governance authority, creating a more pluralistic and accountable governance landscape.

6.4.6. Risks and Limitations of Governance Token Acquisitions

Governance token investing carries unique limitations:

- No legal rights: Unlike equity, tokens don't confer ownership or fiduciary protections.
- Revocable influence: Delegates can be unseated at any time.
- Volatile power: Token price fluctuations can rapidly alter influence.
- Community backlash: Aggressive governance behavior can erode trust.

- Regulatory uncertainty: In some jurisdictions, governance tokens may still be considered securities.

Many funds now conduct governance due diligence before entering a protocol:

- Is the token highly concentrated?
- Are delegation mechanisms transparent?
- Are voting histories and forum participation robust?

Answering these questions is fundamental to properly judge an investment opportunity.

7. Decentralized Governance Models and VC Influence

7.1. Token-Based DAOs

7.1.1. Risks, Delegation Dynamics, and Resilience Mechanisms

Decentralized Autonomous Organizations (DAOs) have emerged as a core governance form in Web3, offering a programmable alternative to traditional corporate control. In their most widespread implementation, DAOs rely on token-weighted voting, whereby the influence of a participant is proportional to the number of governance tokens they hold. This model, while efficient and technically simple, introduces vulnerabilities that challenge the foundational goals of decentralization. In particular, DAOs governed by liquid tokens are highly sensitive to concentration of power, strategic delegation, and low participation rates - dynamics that can erode both legitimacy and resilience.

This section explores the structural risks of token-based DAOs, the role of delegation and soft power, the well-known Uniswap–a16z case as an illustrative example, and current best practices and emerging mechanisms aimed at mitigating governance capture.

7.1.2 Token-Weighted Voting: Design Simplicity, Embedded Fragility

The core principle of token-weighted governance is straightforward: one token equals one vote. The logic follows the shareholder governance model, but without legal ownership or fiduciary responsibility. Token-based DAOs allow participants to vote on proposals ranging from treasury grants to protocol upgrades, fee structures, incentive parameters, and cross-chain deployments.

Despite their promise, token-weighted systems tend to reproduce the very inequalities they were meant to escape. Early token distributions are typically concentrated among founding teams, venture capitalists, and early ecosystem participants. Over time, these entities accumulate long-term influence through either direct token holdings or delegation networks. Furthermore, token liquidity and transferability mean that voting power can be bought, borrowed, or coordinated, sometimes just ahead of crucial votes. This opens the door to governance manipulation, sybil attacks, and vote concentration among economically motivated actors.

The practical risks of this model include:

- Disproportionate VC influence, especially in early-stage DAOs with highly concentrated treasuries
- Low voter turnout, which magnifies the relative power of coordinated whales or delegates
- Short-termism, as investors may vote for strategies that maximize immediate price over long-term sustainability
- No accountability or fiduciary obligations, in contrast with traditional board structures

7.1.3. Delegation and the Rise of Soft Power

To counteract low engagement, many DAOs have adopted delegated voting systems, in which token holders assign their voting rights to a delegate of their choice. Delegation has significant benefits: it

encourages specialization, makes governance more manageable, and allows technically informed or civically engaged individuals to take a leading role in complex protocol decisions.

However, delegation can also mask informal power structures, particularly when used by well-capitalized actors to maintain influence without reputational exposure. Large VCs often delegate their tokens to ecosystem players they trust - or who are dependent on them reputationally or financially.

This dynamic is illustrated in the high-profile Uniswap–a16z governance case. Andreessen Horowitz (a16z), one of Uniswap's earliest and largest backers, received a substantial UNI allocation. In 2023, when the Uniswap DAO voted on whether to deploy Uniswap v3 to Binance Smart Chain using the Wormhole bridge, a16z objected to the proposal - not because of technical concerns, but due to a conflict of interest: it had invested in LayerZero, a competing bridge. While a16z could not vote its entire token stack due to custodial issues, it had previously delegated large amounts of UNI to blockchain clubs at U.S. universities. These delegates ultimately voted in line with a16z's preference, raising concerns about VC influence through proxy and the opacity of delegated governance.

This case catalyzed a broader conversation about how DAOs must distinguish between decentralized participation and coordinated influence, and how token delegation - though well intentioned - can reproduce centralized dynamics behind the veil of decentralization.

7.1.4. Resilience Mechanisms: Designing for Legitimacy and Fairness

To address these issues, DAOs are increasingly experimenting with resilience mechanisms: tools and rules designed to reduce the risks of manipulation, capture, and premature centralization. While these mechanisms vary across protocols, they generally aim to either slow down governance, reduce influence concentration, or increase the friction required to exercise control.

Some of the most prominent resilience mechanisms include:

a. Token Vesting and Lockups

Large token holders - including team members, advisors, and early investors - are often subject to vesting schedules, which delay the transferability or voting utility of tokens. Common structures include a 12-month cliff followed by linear monthly vesting over 24-36 months. Lockups are enforced through smart contracts or off-chain agreements, limiting the ability of capital-heavy actors to dominate governance from day one.

b. Proposal Thresholds and Quorum Rules

To prevent frivolous or malicious proposals, DAOs often require proposers to hold a minimum number of tokens and enforce a minimum quorum of votes for proposals to pass. For example, Compound requires 25,000 COMP to submit a proposal and a 400,000 COMP quorum to enact changes. While thresholds promote signal over noise, they also risk entrenching existing power if not calibrated carefully.

c. Time Delays and Veto Windows

Once a proposal passes, some protocols implement execution delays, giving the community time to review, contest, or counteract decisions before they go live. This buffer, typically 24 to 72 hours, serves as a failsafe against rushed or manipulated governance outcomes. In some cases, emergency veto powers

- managed by multisig signers or governance stewards - can pause or reverse execution in extreme circumstances.

d. Governance Token Design

At the heart of every token-based DAO lies a crucial question: *who should have the power to decide?* The answer depends not only on how governance processes are structured, but also on how the governance token itself is designed. Token design is not just a technical parameter - it is a political and economic choice. It determines how power is distributed, whether it can be bought, how it evolves over time, and how aligned it is with long-term contributors rather than short-term speculators.

In early DAOs, governance tokens were often transferable, liquid, and distributed primarily through early fundraising rounds or public sales. This simplicity made adoption fast but also left protocols vulnerable to whale dominance, plutocracy, and value extraction by transient actors. As a result, Web3 designers have begun experimenting with alternative governance token models that better protect against capture and promote genuine participation.

New DAO architectures are also rethinking the token itself. Innovations include:

- Non-transferable governance tokens, like those used in Optimism's Citizens' House, to prevent market-based capture
- Quadratic voting, where marginal voting power decreases with token amount, rewarding breadth over depth of participation
- Vote caps, which limit the maximum influence of any single wallet
- Dual-token systems, where one token is used for economic utility (e.g., staking or yield), and another for governance

These designs aim to separate wealth from power - or at least reduce the rate at which capital can be converted into unilateral influence.

Below, we explore the current four major directions in governance token innovation:

d.1. Non-Transferable and Identity-Linked Governance Tokens

To prevent governance power from becoming a commodity that can be purchased or aggregated, some protocols have introduced non-transferable tokens - sometimes called *soulbound tokens* - that are linked to a unique identity, contribution, or reputation.

A leading example is Optimism's Citizens' House, which governs public goods funding through identity-based voting badges. These badges are awarded - not bought - and cannot be sold or traded. In doing so, the protocol separates governance from capital and ties influence to community legitimacy.

This model draws inspiration from civic institutions: power is based on participation and qualification, not economic stake. While it raises questions around identity verification, sybil resistance, and scalability, it offers a promising path toward more inclusive and capture-resistant governance.

d.2. Quadratic Voting and Participation-Weighted Influence

Quadratic voting (QV) attempts to correct the linear relationship between tokens and votes by introducing diminishing returns to scale. Instead of each token granting one vote, QV requires participants to spend the *square* of the number of votes they want. For example, to cast 4 votes, you need 16 tokens.

This design:

- Amplifies small contributors with high conviction
- Penalizes large holders who attempt to dominate votes
- Encourages collective deliberation and funding diversity

Quadratic voting is most famously implemented in Gitcoin Grants, where public goods funding is distributed based not on total capital raised, but on breadth of support. Projects with many small donors are prioritized over those with a few large backers.

Despite its benefits, QV requires robust sybil resistance (identity verification mechanisms), otherwise whales can simply split their tokens across wallets. Protocols like Gitcoin address this through Gitcoin Passport, which aggregates identity signals (e.g., GitHub, Twitter, ENS) to assess legitimacy.

d.3. Vote Caps and Rate-Limiting Mechanisms

Another approach is to cap the influence any single wallet or entity can exert, regardless of how many tokens it holds. These mechanisms may take the form of:

- A maximum vote weight per address (e.g., no more than 5% of total votes)
- Rate-limiting rules that restrict how often a large holder can vote or propose
- Randomized voter selection from eligible participants (used in some quadratic lotteries)

Vote caps aim to protect against coordinated takeovers or whale attacks, especially in low-turnout DAOs. While effective in theory, they can be gamed through wallet splitting or delegation unless paired with robust identity or governance tracking systems.

As of 2025, few major DAOs implement hard caps at the protocol level - but several include them informally in off-chain voting platforms (e.g., Snapshot, Tally), or through community norms around abstention and conflict-of-interest disclosures.

d.4. Dual-Token and Hybrid Governance Models

To separate economic and political power, some protocols adopt dual-token systems, in which one token represents value accrual (e.g., staking, yield) and another represents governance rights. This reflects a fundamental distinction: who benefits from the protocol, versus who decides its direction.

Examples include:

- Protocols that distribute "governance-only tokens" to long-term contributors or verified users (e.g., Aragon Voice)
- Systems where governance tokens are earned, not bought, through activity, proposals, or community participation

- Approaches that combine equity + token voting models, where governance is shared between legal shareholders and protocol participants (e.g., some DAO-firm hybrids)

Hybrid models also allow for multi-house governance (as seen in Optimism), where separate chambers - one capital-based, one identity-based - govern different areas of protocol control (e.g., treasury, tech roadmap, public goods).

These systems are more complex to implement, and often require off-chain identity verification or delegated oversight - but they offer a layered, resilient governance architecture, more closely resembling institutional checks and balances.

d.5 Trade-Offs and Open Questions

Each governance token design comes with trade-offs between efficiency, decentralization, sybil resistance, and user experience.

Design Feature	Benefit	Risk or Trade-Off
Non-transferable tokens	Prevents plutocracy, aligns with merit	Limits market liquidity and delegation
Quadratic voting	Amplifies collective voice	Vulnerable to sybil attacks
Vote caps	Prevents whale domination	Easy to bypass without identity tracking
Dual-token models	Separates economics from governance	Increases complexity and coordination cost

Table 1. Benefits and Risks of governance token designs.

7.2. Council-Based Governance

Hedera Hashgraph, Institutional Voting, and the Limits of Tokenless Decentralization

While most blockchain protocols experiment with token-based governance as their primary mechanism for decision-making, a distinct group of networks adopts an alternative path: council-based governance. In this model, governance power is not distributed among token holders but instead concentrated in a designated group of entities, often composed of large institutions, universities, or reputable corporations. These actors are granted equal voting rights, and collectively make decisions about protocol upgrades, treasury management, fee structures, and broader strategic direction.

Council-based governance is not decentralized in the tokenomic sense, but it seeks to achieve decentralization through diversity, transparency, and accountability among well-known participants. It aims to bring stability, legal clarity, and professional oversight to blockchain ecosystems - often at the expense of openness and grassroots participation. This section explores the governance architecture of Hedera Hashgraph, the best-known example of council-led blockchain governance, and reflects on the broader implications and trade-offs of non-token voting systems.

7.2.1. The Hedera Model: Governance Through a Global Council

Hedera Hashgraph is a public distributed ledger that uses a unique consensus mechanism called hashgraph, rather than a traditional blockchain. From its inception, Hedera has chosen not to implement token-based governance. Instead, it is governed by a council of up to 39 global organizations, including major enterprises such as Google, IBM, Boeing, Deutsche Telekom, Nomura, and the London School of Economics.

Each council member holds equal voting power, regardless of economic contribution, technical stake, or HBAR token holdings. Members are selected for their global reach, sectoral diversity, and operational independence. The council is term-limited, meaning that participation is temporary and regularly rotated to avoid long-term entrenchment. Council members are responsible for making decisions on:

- Network upgrades and software improvements
- Fee structures and protocol parameters
- Treasury allocations and HBAR economics
- Legal and compliance policies
- Strategic direction and roadmap alignment

Importantly, the council does not control network consensus - the hashgraph consensus layer is separate. However, it does govern the rule-set and business logic that determine how the network evolves.

To preserve accountability, Hedera's governance processes are transparent and auditable. Council meeting minutes are published regularly, and major decisions are subject to public review. This transparency is intended to offer a form of institutional legitimacy - an anchor point for users, developers, and regulators looking for predictability and professionalism.

7.2.2. Why Council-Based Governance?

The choice to implement council-based governance is not simply a philosophical preference - it is a deliberate institutional design decision, often driven by three primary motivations:

a. Legal and Regulatory Clarity

Many blockchain protocols struggle to maintain compliance with securities laws, data regulations, or platform liability standards. Council-based governance offers a centralized but accountable structure that can interface with governments, maintain internal compliance, and provide clarity in areas where DAOs face ambiguity. Hedera, for example, has been able to partner with enterprises and institutions in highly regulated industries because of this trust-building architecture.

b. Institutional Trust and Adoption

Protocols targeting enterprise or public-sector use cases often require guarantees that decentralized, anonymous actors cannot provide. A fixed governance council composed of known legal entities provides contractual continuity, reputational assurance, and conflict resolution mechanisms. This is essential when building infrastructure for cross-border payments, supply chains, or identity systems.

c. Operational Stability and Long-Term Planning

Council governance provides a stable planning horizon, allowing for multi-year initiatives, well-funded R&D, and cohesive decision-making. Token-based DAOs, by contrast, can suffer from strategic inconsistency, populist incentives, or underfunded governance infrastructure. By curating a council of

long-term stakeholders, protocols can engage in governance as stewardship, rather than as reactive polling.

7.2.3. Advantages of Non-Token Voting Systems

Council-based governance offers several important advantages over token-based models - especially in terms of robustness, clarity, and coordination.

Equal Voting Power, Regardless of Capital

In Hedera's model, every council member has exactly one vote. This avoids the "one token, one vote" problem, where early investors and whales can control protocol outcomes by sheer economic weight. Equal voting power promotes diverse perspectives, levels the playing field across sectors, and reduces the temptation for governance capture.

Identity-Based Accountability

Council members are public, reputationally exposed, and legally responsible for their governance actions. This creates a strong incentive for thoughtful participation and responsible decision-making and avoids the opacity of token delegation or anonymous voting behaviors.

Expertise and Technical Competence

Unlike DAOs where voters may lack the time or capacity to review complex proposals, council members are selected for their ability to understand and contribute to protocol governance. Their participation can be structured, well-informed, and tied to measurable KPIs.

Predictable Governance Cycles

Because governance is conducted through scheduled council meetings with formal agendas and minutes, the process is far more structured and reliable than asynchronous forum discussions and token snapshot voting. This allows for long-term strategy and better alignment with stakeholders.

7.2.4. Limitations and Critiques of Council Governance

Despite its strengths, council-based governance also faces significant criticisms, particularly from proponents of decentralized finance and permissionless systems.

Lack of Grassroots Participation

The most obvious limitation is the absence of broad community input. Users, developers, or holders of the protocol's native token (HBAR, in Hedera's case) do not have formal voting rights. This creates a representational gap between the protocol's decision-makers and its users.

Centralization of Power

While the council model spreads control across multiple entities, it remains non-permissionless. Entry into the council is selective and controlled, and decisions are made behind institutional doors, even if transparently reported afterward. This opens the model to criticisms of elitism or opaque deal-making.

Difficult Exit and Fork Paths

In a fully decentralized, token-based system, dissatisfied communities can fork the code and governance system. In a council-based model, network governance is tightly linked to the institutional council, making it harder for dissenting actors to break away or reclaim control. This can create friction around accountability and change management.

Risk of Regulatory Capture or Collusion

While council members are individually reputable, they may share institutional interests that lead to converging biases - e.g., toward compliance-heavy design choices or risk aversion. There is also the risk that external regulators could coerce or pressure council members, undermining network neutrality.

7.2.5. A Complement, Not a Competitor

Council-based governance, as exemplified by Hedera Hashgraph, does not aim to compete with token-based DAOs - it serves a different institutional niche. It is particularly well-suited to use cases where predictability, legal clarity, and reputational trust are prerequisites for adoption. It provides a model for how blockchain protocols can engage with regulated industries, build multi-stakeholder governance, and develop infrastructure that spans borders and legal systems.

However, its trade-offs must be acknowledged. Council models sacrifice openness for stability, and decentralization for deliberation. They depend on the quality, diversity, and accountability of the council itself. Over time, the best implementations may be hybrid systems - combining the efficiency of token governance with the stability and structure of council oversight, allocating different domains of control to different governance bodies.

As the governance landscape continues to evolve, council-based systems offer a valuable template for network design under constraint, and for imagining how blockchain technologies can achieve institutional trust without collapsing into unchecked plutocracy.

7.3. Protocol-Level On-Chain Governance

Conviction Voting, Vote Escrow, Identity, and Code as Institutional Design

As DAOs mature, the limitations of simple token-weighted governance - namely its vulnerability to capital concentration, disengaged voting, and sybil manipulation - have become increasingly apparent. In response, Web3 designers are pioneering alternative voting models and decision-making frameworks that attempt to decouple influence from wealth, incentivize commitment, enhance resilience, and broaden participation.

This section reviews a range of governance innovations currently being tested across major protocols. While none of these models offer a perfect solution, each represents an important shift in how blockchain communities define voice, legitimacy, and control.

7.3.1. Conviction Voting (Polkadot, Kusama)

Conviction voting ties voting power to time commitment. Instead of granting one vote per token, this model rewards users who are willing to lock their tokens for longer periods, aligning influence with long-term conviction rather than short-term capital.

Implemented in the Polkadot and Kusama ecosystems, conviction voting allows participants to voluntarily lock up DOT or KSM tokens for varying durations, increasing their voting power exponentially. A user who locks their tokens for one week might have 2× voting power, while a one-year lock could yield up to 32× weight. This system is designed to:

- Reduce flash governance, where whales acquire voting power temporarily to pass opportunistic proposals
- Reward committed contributors, who are invested in the protocol's long-term health
- Slow down volatility, by anchoring governance power in temporal commitment

The model is enforced at the protocol level, making it tamper-resistant and programmable. However, it can still be gamed if token lockup is automated or subsidized by centralized actors, and it may discourage participation from newer users or liquidity-constrained voters.

7.3.2. Vote Escrow Models (Curve veCRV, Balancer veBAL)

One of the most influential governance innovations in DeFi is the vote escrow model, pioneered by Curve Finance with veCRV ("vote-escrowed CRV"). In this model, users lock their tokens for a fixed period (up to 4 years) to receive voting rights and economic incentives. Their voting power decays over time unless they re-lock.

This model has two main effects:

- It turns governance into a long-term commitment, not a tradeable right
- It aligns governance power with protocol loyalty, not market speculation

Balancer adopted the same model via veBAL, with similar mechanics and boosted liquidity incentives. These systems reward users who are "in it for the long haul," and have proven effective at aligning liquidity provision, governance participation, and token value.

Vote escrow also introduces complex dynamics - such as the infamous "Curve Wars", where protocols compete to accumulate veCRV votes to direct emissions toward their pools. While this creates strategic engagement, it can also incentivize bribery, lobbying, and governance cartels.

7.3.3. Dual Governance Chambers (Optimism's Token House and Citizens' House)

The Optimism Collective introduced one of the most structurally ambitious governance designs in Web3: a bicameral (two-house) governance model, inspired by constitutional democracies. It separates economic control from civic governance.

- The Token House is composed of OP token holders and governs protocol upgrades, incentive programs, and technical parameters.
- The Citizens' House is made up of individuals granted non-transferable "soulbound" citizenship badges, who vote on public goods funding and community allocation decisions.

This structure introduces purpose-specific voting rights: capital governs capital, while public interest governs public goods. By doing so, Optimism acknowledges that different decisions require different legitimacy bases.

The Citizens' House uses identity-based voting, decoupled from token ownership, and relies on social norms, reputation, and curated participation. This model:

- Reduces plutocracy, especially in funding decisions
- Elevates long-term contributors and public goods advocates
- Enables hybrid governance logic, balancing financial and social value

While still in early development, this dual-chamber system sets a powerful precedent for polycentric governance in Web3.

7.3.4. Quadratic Voting and Gitcoin Grants

Quadratic voting (QV) addresses wealth concentration by penalizing large vote accumulations and amplifying small contributions. Instead of linear cost, voting weight grows with the square of the votes cast, meaning:

- Casting 1 vote costs 1 token
- Casting 4 votes costs 16 tokens
- Casting 10 votes costs 100 tokens

This non-linear structure is most famously applied in Gitcoin Grants, where matching funds are distributed based on the number of contributors, not the total donated. A project with 1,000 donors giving $1 each receives more funding than one with 1 donor giving $1,000.

Quadratic Voting:

- Incentivizes broad community participation
- Mitigates whale dominance
- Encourages diversity of support

However, it is vulnerable to sybil attacks, as users can fake many identities to simulate popular support. Gitcoin addresses this through Gitcoin Passport, an identity aggregation tool that assigns legitimacy scores based on cross-platform credentials (e.g., ENS ownership, Twitter presence, GitHub contributions).

Quadratic voting is not yet widely used for protocol-level governance (e.g., parameter changes or upgrades), but it excels in funding allocation, ranking systems, and signal voting contexts.

7.3.5. Reputation-Based and Contribution-Weighted Voting (Radicle, Aragon v1)

In an attempt to move beyond capital, several early DAOs experimented with reputation-based governance, where voting power is earned through contribution, not purchase. Projects like Radicle, Aragon (v1), and early DAOstack pilots weighted votes based on:

- GitHub contributions
- Forum activity
- Proposal authorship
- Bounties completed

The core idea is that those who build the protocol should help govern it. Unlike token voting, which can be passive or speculative, reputation governance requires visible, trackable engagement.

However, these systems struggled to scale, due to:

- Subjectivity in measuring contributions
- Centralization risk in assigning reputation
- Complexity in integrating with smart contracts

Despite these hurdles, reputation governance remains a long-term aspiration for many DAOs seeking to evolve from purely economic to meritocratic or pluralistic systems.

7.3.6. Governance by Code (Stacks' Clarity Contracts)

Some protocols go beyond voting by encoding governance rules directly into the smart contract logic. The clearest example is Stacks, a Bitcoin Layer-2 network governed by the Clarity programming language - a decidable, transparent smart contract language designed specifically for predictable execution.

Stacks enforces key governance functions through on-chain rules, not votes:

- Protocol upgrades require predefined quorum + signaling mechanisms
- Treasury disbursements follow codified eligibility and timing logic
- Dispute resolution oracles are pre-integrated into contract logic

This "governance by code" reduces ambiguity and manual intervention, providing a strong formal guarantee against manipulation. While less flexible than DAO-style voting, it excels in environments that prioritize security, compliance, and stability.

The trade-off is reduced adaptability. Any changes to governance rules require hard-coded upgrades, making governance more predictable but less dynamic.

7.3.7. Sybil Resistance and Identity-Based Voting (Gitcoin Passport, Optimism Badges)

Many of the governance models above - especially those based on quadratic voting, non-transferable tokens, or contribution scoring - rely on sybil resistance: the ability to distinguish between real users and fake or duplicated identities.

In Web3, sybil resistance is typically addressed via identity aggregation frameworks that do not compromise privacy. For example:

- Gitcoin Passport aggregates on-chain and off-chain identity signals to build a "trust score", while maintaining user pseudonymity.

- Optimism badges are non-transferable tokens issued to real contributors, granting governance privileges in the Citizens' House.
- Other projects use BrightID, Proof of Humanity, or ZK identity attestations to limit vote inflation.

Identity-based systems are still experimental, and raise important ethical questions around inclusion, anonymity, and surveillance. However, they represent a critical foundation for any governance model that wishes to move beyond token ownership as the sole marker of legitimacy.

7.4. Cross-Protocol Governance Map

As decentralized governance evolves, leading protocols have begun to diverge in structure, philosophy, and execution. Some prioritize speed and token-holder control (Uniswap, Compound), while others introduce hybrid systems that attempt to balance capital and community (Optimism). Still others, like Arbitrum, face governance bottlenecks that reveal critical tensions between decentralization and operational coherence.

This section compares the governance models of Uniswap, Compound, Optimism, and Arbitrum, examining how each protocol structures participation, delegates power, and protects itself from manipulation or stagnation. The goal is not to crown a winner, but to highlight what works, what does not, and why resilience in governance design increasingly depends on context, pluralism, and intentional architecture.

7.4.1. Governance Structures at a Glance

Protocol	Governance Token	Proposal Mechanism	Execution	Delegation	Additional Features
Uniswap	UNI	On-chain (Tally)	Timelock executor	Yes	No formal council or veto; delegation is widespread
Compound	COMP	On-chain (Governance module)	Autonomous executor	Yes	Strong quorum + threshold system; early DeFi standard
Optimism	OP	Dual House: Token House & Citizens' House	Multisig + Council	Yes (Token House)	Identity-based governance for public goods (Citizens' House)
Arbitrum	ARB	On-chain (Snapshot + DAO contracts)	Security Council + DAO voting	Yes	High treasury control; recent proposal backlash

Table 2. Governance Structure Overview of Uniswap, Compound, Optimism and Arbitrum protocols.

7.4.2. Uniswap: Technically Elegant, Politically Fragile

Uniswap was one of the earliest DeFi protocols to experiment with fully on-chain, token-based governance using the UNI token. While its governance architecture is technically sound, the protocol has faced recurring criticism for concentration of power and low voter engagement.

- Strengths: Simplicity, transparency, and widespread token distribution.
- Weaknesses: High quorum (40M UNI), low participation rates, and delegation dominance by VCs - notably a16z, whose influence over certain votes (e.g., Wormhole vs. LayerZero bridge) raised red flags about proxy control and soft power.
- What doesn't work: Without active users and independent delegates, even decentralized systems become oligarchic in practice. UNI remains broadly distributed, but governance activity is low and often reactive.

7.4.3. Compound: Technocratic and Consistent, But Inertial

Compound set the gold standard for early DeFi governance: COMP token holders vote directly on proposals using an autonomous on-chain executor that applies changes automatically upon approval. This structure is clear, modular, and tamper-resistant.

- Strengths: High proposal thresholds (25K COMP) and quorum (400K COMP) ensure signal over noise. Compound has a technocratic culture, with developers and protocol politicians writing detailed proposals (CIPs).
- Weaknesses: Participation is limited to a small group of technically proficient actors. Average users often feel disconnected from governance. The system is also relatively slow-moving due to procedural friction.
- What works: A clear process, consistent standards, and effective use of delegation.
- What does not: Inertia. Despite sound mechanics, community engagement is modest and path dependency is high.

7.4.4. Optimism: Pluralistic Governance for a Multi-Stakeholder World

Optimism introduced a radically different model with its dual governance chambers:

- The Token House governs protocol upgrades and incentive distribution
- The Citizens' House manages public goods funding, based on non-transferable soulbound badges

This design reflects an explicit division of economic and civic power, with the goal of creating sustainable coordination at scale.

- Strengths: Role-specific governance domains reduce capture risks. Optimism's funding rounds are transparent, inclusive, and actively debated. Gitcoin Passport integration helps with sybil resistance in Citizens' House.
- Weaknesses: Still early and difficult to scale - especially the identity infrastructure and badge issuance. Requires strong governance curation.
- What works: Clear separation of powers, diverse legitimacy sources, and public goods alignment.
- What does not: Complexity creates participation friction, especially for non-technical users unfamiliar with dual-layered voting.

7.4.5. Arbitrum: Treasury Blowback and Governance Under Pressure

Arbitrum's governance is token-based (ARB), but also mediated by a Security Council (multisig signers) and DAO-controlled treasury. In 2023, Arbitrum's DAO faced backlash after a $1 billion treasury allocation was effectively announced before DAO approval, revealing a governance process that was decentralized in form, but not in execution.

- Strengths: Strong ecosystem participation and well-capitalized treasury. Use of on-chain voting with public documentation.
- Weaknesses: Top-down decision-making masquerading as community-driven. The DAO rejected initial proposals and demanded better transparency.
- What works: Treasury power activated community debate and made governance visible.
- What does not: Lack of process discipline undermined trust; formal control didn't match informal decision-making.

7.4.6. What Works - Across the Board

Despite their differences, a few common design principles emerge as successful:

1. Clear and enforceable process logic
   → Compound and Uniswap benefit from robust, on-chain procedures that reduce ambiguity.
2. Delegation frameworks that include transparenc
   → Delegates in Compound and Optimism often post rationales and vote histories.
3. Purpose-specific governance domain
   → Optimism's dual houses offer a promising model for managing different coordination goals (e.g., economic vs civic).
4. Quorum thresholds that balance inclusion with protection
   → High thresholds (Compound) prevent frivolous governance, while lower barriers (Optimism Token House) invite participation.

7.4.7. What Doesn't Work - Key Governance Failures

Some features consistently lead to governance fragility:

1. Unmanaged delegation opacity
   → Uniswap's delegation to university clubs (via a16z) revealed soft influence mechanisms with no formal checks.
2. Treasury discretion without process
   → Arbitrum's $1B vote triggered crisis because the DAO vote appeared symbolic, undermining procedural trust.
3. Incentivized participation without identity anchoring
   → Gitcoin and Optimism show that public goods voting needs sybil resistance, or else becomes vulnerable to strategic manipulation.
4. Overreliance on token liquidity
   → When voting power is fully liquid, short-term actors can rent control, especially during low-attendance periods.

7.4.8. Governance is Architecture, not Optics

Governance is not about symbolism - it is about institutional design. Protocols that succeed over the long term are those that align:

- Decision rights with domain-specific legitimacy
- Voting mechanisms with clear incentives and accountability
- Governance transparency with enforceable rules

There is no perfect model. What matters is design intentionality: understanding who should decide what, when, and how - and structuring systems that scale trust, reduce friction, and evolve with the protocol's maturity.

As DAOs mature, governance must move beyond token-based entitlements and embrace pluralistic systems that reflect social, technical, and economic complexity. The comparative map offered here is a starting point for that evolution.

7.5. Resilience Mechanisms

As token-based governance spreads across Web3, the need for resilience mechanisms - structures that protect DAOs from manipulation, apathy, and overcentralization - has become increasingly urgent. While early DAO models often relied on simple token-weighted voting, this framework has proven vulnerable to a variety of risks: plutocratic control by early investors, voter fatigue, procedural deadlocks, and opaque delegation. In response, leading protocols are experimenting with more pluralistic, adaptive, and transparent governance models that aim to balance efficiency with inclusion, and decentralization with reliability.

This section explores the key mechanisms emerging across the DAO ecosystem to enhance governance resilience. It highlights specific design choices such as quadratic voting, dual-chamber systems, vesting schedules, delegation transparency, and veto safeguards, and concludes with lessons from both failed and enduring governance architectures.

7.5.1. Quadratic Voting and Identity Anchoring

A core challenge of token governance is that it scales linearly with capital. This creates a system where those with the deepest pockets have the most power - regardless of alignment or contribution. Quadratic voting (QV) attempts to rebalance this by making each additional vote more expensive than the last, thus amplifying smaller participants and penalizing vote concentration.

In practice, QV has been most effectively deployed in funding contexts, especially via Gitcoin Grants, where matching funds are distributed based on the number of unique donors rather than the total value donated. However, its governance potential goes beyond grant-making. Quadratic voting:

- Encourages wide participation from long-tail contributors
- Mitigates the dominance of large token holders
- Signals community support more effectively than raw vote counts

QV systems do, however, depend on sybil resistance. Without robust identity frameworks, QV can be gamed through fake wallets. Solutions like Gitcoin Passport or BrightID attempt to anchor voting rights

in provable, pseudonymous identity - an essential prerequisite for making these voting mechanisms resilient.

7.5.2. Dual-Chamber Governance: The Optimism Model

Optimism's bicameral governance offers one of the most sophisticated attempts to segment governance power across distinct stakeholder groups. The Token House, composed of OP holders and delegates, governs core protocol decisions, such as upgrades and incentive programs. In contrast, the Citizens' House is a soulbound, non-transferable identity layer responsible for retroactive public goods funding.

This separation of powers introduces role-specific legitimacy:

- Token holders manage economic infrastructure, where stake and capital are relevant
- Citizens govern social capital and funding decisions, where alignment and trust matter more than tokens

The dual-chamber system mitigates the risk of capital-driven governance capture, particularly for functions - like public goods allocation - that depend on ethical judgment and ecosystem alignment. It also opens space for non-investor participants, such as developers, educators, and public goods advocates, to gain meaningful influence through non-financial contributions.

While still in development, Optimism's model demonstrates that governance resilience is often a question of functional differentiation, not just voting mechanics.

7.5.3. Vesting Schedules and Temporal Lockups

One of the most effective defenses against speculative or manipulative governance is time. By ensuring that large token allocations - particularly to insiders or VCs - are subject to vesting schedules and lockups, DAOs can reduce short-term opportunism and better align governance incentives with long-term value creation.

For example:

- In many protocols, core team and investor tokens are subject to multi-year vesting, during which voting rights are limited or restricted.
- Some DAOs implement time-locked governance for critical actions, requiring a waiting period between proposal passage and execution (e.g., Compound's Timelock).
- Other designs include progressive governance activation, where voting power increases with time held (as in conviction voting) or decays unless re-committed (as in veCRV models).

These tools make governance power less liquid, and therefore less susceptible to opportunistic accumulation or vote-buying. They also enforce temporal skin in the game, rewarding those who remain invested in the protocol's future.

7.5.4. Delegation Transparency and Meta-Governance

Delegation is a powerful mechanism in token governance, enabling passive holders to transfer their voting rights to more active or informed participants. However, without transparency, it can become a channel for stealth control - particularly when VCs delegate to aligned actors or create indirect influence networks.

Protocols have responded by developing delegation dashboards (e.g., Tally, Agora, Karma) that make voting histories, rationale statements, and delegate profiles public. This improves accountability, discourages shadow governance, and empowers token holders to make informed delegation decisions.

Meta-governance tools now track:

- Delegate voting consistency and attendance
- Conflicts of interest or affiliated proposals
- Contribution to governance discussions and working groups

A mature delegation ecosystem increases participation without compromising integrity - provided that influence flows are traceable, revocable, and based on performance.

7.5.5. Veto Powers, Guardians, and Emergency Committees

Another layer of resilience comes from mechanisms designed to prevent catastrophic or malicious governance actions. These include:

- Veto councils or guardian multisigs with limited-use override powers
- Emergency delay mechanisms, allowing the community to review or cancel proposals before execution
- Minimum quorum and proposal thresholds, ensuring that only widely supported initiatives pass

These tools are controversial - seen by some as a step backward toward centralization - but they serve an important transitional function. When designed carefully, such fail-safe mechanisms can be gradually phased out as a DAO matures and its social contract solidifies.

Protocols like Arbitrum (via its Security Council) and MakerDAO (via its Emergency Shutdown Module) have demonstrated the pragmatic value of non-token safeguards during periods of instability or low voter turnout.

7.5.6. Lessons from Failure and Resilience

The Web3 ecosystem now offers a diverse set of case studies in governance resilience - and failure.

Failure modes include:

- Uniswap's a16z delegation strategy, which, while technically decentralized, concentrated influence among VC-aligned university clubs, sparking a backlash around "protocol capture"
- Arbitrum's rushed treasury transfer, where a DAO vote was overridden by a pre-emptive Foundation action, undermining trust in the DAO's authority
- Curve's bribery dynamics, where vote escrow models created a market for vote-buying and incentive distortion

Resilient models demonstrate:

- Compound's clear quorum and timelock architecture, which has withstood multiple governance cycles without major procedural breakdown
- Optimism's dual-chamber structure, which intentionally decentralizes power and invites new stakeholders into governance
- Gitcoin's evolution, which blends quadratic voting, identity verification, and open deliberation to balance inclusion and trust

Perhaps the most important lesson is that governance cannot be an afterthought. Protocols that invest early in resilient, pluralistic, and transparent governance are more likely to maintain legitimacy - and attract committed communities - over time.

8. Crypto-VC Investment Networks

8.1 Who are the Top Investors?

The following lists illustrate the top 20 investors, reported by CryptoRank on the 8th of September 2025 and ranked, respectively, by number of projects in the investor's portfolio and retail ROI, calculated based on the IDO, IEO or ICO data of the projects reported per investor.

8.1.1 Top 20 Investors by Portfolio

Name	Tier	Portfolio	Retail ROI
Coinbase Ventures	1	461	4.19x
Animoca Brands	3	455	1.77x
AU21 Capital	3	290	0.28x
NGC Ventures	3	281	7.40x
HashKey Capital	1	276	13.79x
Shima Capital	2	267	0.40x
Digital Currency Group (DCG)	2	251	403.63x
LD Capital	3	229	105.07x
Alameda Research		229	158.65x
Pantera Capital	1	228	235.08x
The Spartan Group	1	227	13.41x
OKX Ventures	2	214	11.69x
Polychain Capital	1	213	24.72x
x21 Digital	3	207	0.05x
CMS Holdings	2	195	13.06x
ExNetwork Capital	3	194	0.77x
GSR	2	191	19.82x
GBV Capital	2	189	0.72x
ZBS CAPITAL	3	186	0.07x
Andreessen Horowitz	1	183	794.30x

Figure 13. Top 20 Crypto VC Investors by Portfolio Size. Ranking of firms by number of portfolio projects, updated the 8th September 2025 Source: CryptoRank.

8.1.2 Top 20 Investors by Retail ROI

Name	Tier	Portfolio	Retail ROI
M31 Capital	4	9	4651.40x
8 Decimal Capital	4	8	3493.96x
Winklevoss Capital	3	26	3489.61x
Boost VC	2	40	2792.52x
Union Square Ventures	2	48	2016.64x
1confirmation	2	43	1751.99x
Paradigm	1	109	1402.84x
KR1	3	31	1268.68x
Lecca Ventures	4	7	1084.66x
FL Foundation	5	1	1084.66x
Electric Capital	2	98	1078.40x
Placeholder Ventures	3	54	1075.24x
CMT Digital	2	123	999.24x
Passport Capital	4	2	974.87x
Galaxy	1	139	940.79x
Fabric Ventures	2	80	875.37x
Andreessen Horowitz	1	183	794.07x
Maven 11 Capital	2	89	699.40x
SNZ Holding	3	115	424.17x
Three Arrows Capital		72	417.05x

Figure 14. Top 20 Crypto VC Investors by Retail ROI. Ranking of firms by realized ROI, updated the 8th September 2025 Source: CryptoRank.

8.1.3 Nature of the Funds

The investor base in crypto VC can broadly be divided into crypto-native firms, of which the majority of our rankings consist of, and generalists VCs. Specifically, in the former category we find:

- 1confirmation
- 8 Decimal Capital
- Alameda Research
- Animoca Brands
- AU21 Capital
- Boost VC
- CMS Holdings
- CMT Digital
- Coinbase Ventures
- Digital Currency Group
- Electric Capital
- ExNetwork Capital
- Fabric Ventures
- Galaxy
- GBV Capital
- GSR
- HashKey Capital
- KR1
- LD Capital
- Lecca Ventures
- M31 Capital
- Maven 11 Capital
- NGC Ventures
- OKX Ventures
- Pantera Capital
- Paradigm
- Placeholder Ventures
- Polychain Capital
- Shima Capital
- SNZ Holding
- The Spartan Group
- Three Arrows Capital
- x21 Digital
- ZBS Capital

While generalists VCs figuring among the top investors are:

- Winklevoss Capital
- Union Square Ventures
- Andreessen Horowitz
- Passport Capital
- FL Foundation

8.2 Which Sectors Do They Fund?

8.2.1 Focus Area Ranking by Portfolio

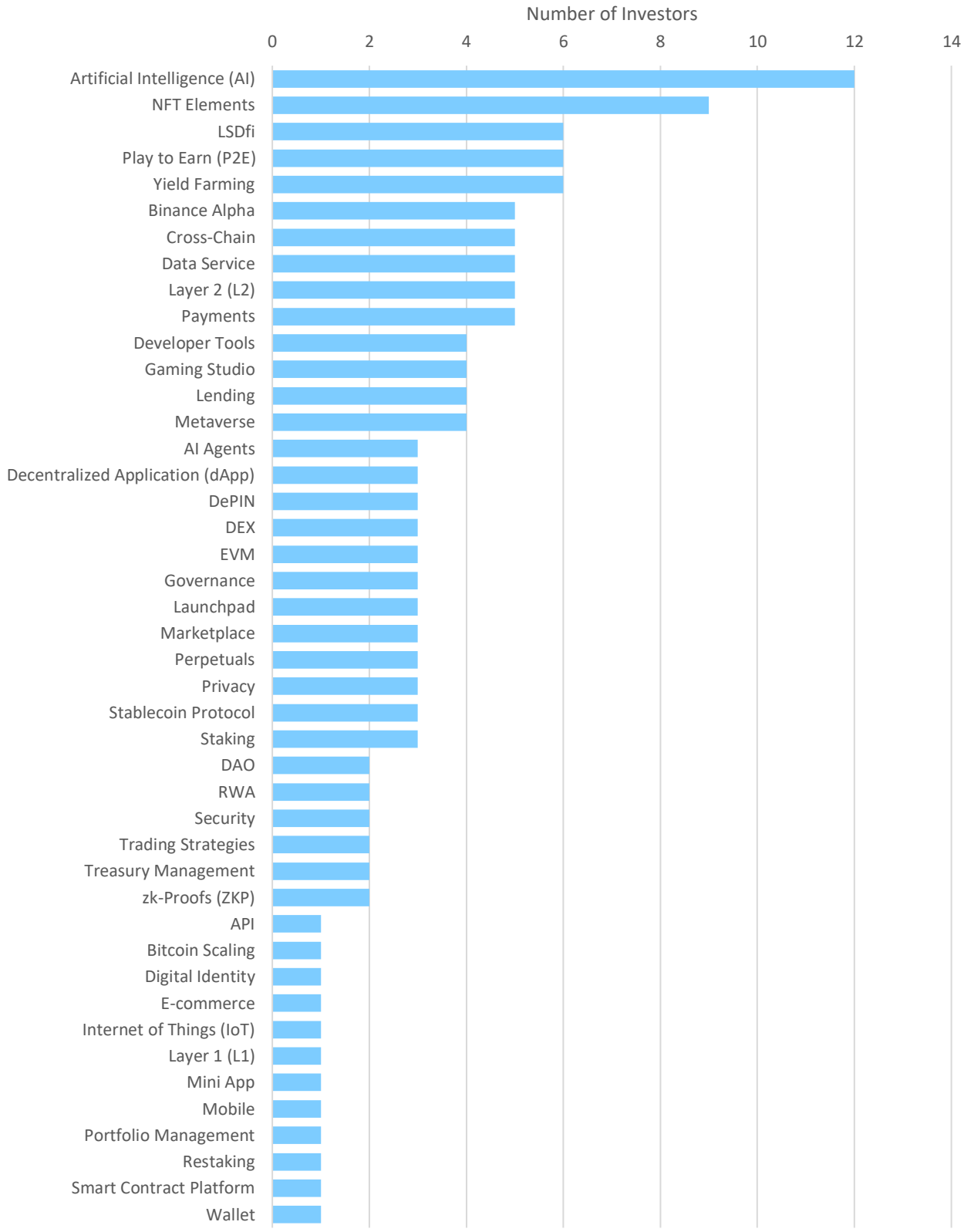

Figure 15. Focus Areas of the Top 20 VC Investors by Portfolio. Updated the 8th September 2025. Source: CryptoRank.

The analysis of the top 20 investors ranked by portfolio shows a strong concentration in Artificial Intelligence and NFT-related projects, with over half of these investors allocating to at least one of the two. Other categories with notable representation include LSDfi, Play-to-Earn, Yield Farming, and Binance Alpha, all appearing in the portfolios of 5–6 investors. A second cluster of areas (including Cross-Chain solutions, Data Services, Layer 2, and Payments) attracts moderate attention. Beyond this, the distribution spreads widely across many smaller niches, from Governance to Bitcoin Scaling, indicating broad experimentation but less consensus.

Key to focus areas:

- Artificial Intelligence (AI): Startups applying machine learning and AI models to blockchain, ranging from AI-driven trading, data analytics, to autonomous agents.
- NFT Elements: Platforms and tools supporting non-fungible tokens, including marketplaces, infrastructure for minting/trading, and specialized NFT utilities.
- LSDfi (Liquid Staking Derivatives Finance): Protocols built on liquid staking tokens, enabling them to be reused in lending, yield, and DeFi strategies.
- Play-to-Earn (P2E): Gaming models where users earn crypto or NFTs as rewards for in-game activity.
- Yield Farming: Strategies and platforms that maximize returns by allocating liquidity across multiple DeFi protocols.
- Binance Alpha: Projects tied to Binance's ecosystem (e.g., early-stage support, incubations, or strategic verticals linked to Binance).
- Cross-Chain: Infrastructure that connects multiple blockchains, enabling asset or data transfer across different networks.
- Data Service: Oracles, data availability layers, and analytics providers ensuring reliable on-chain/off-chain information flow.
- Layer 2 (L2): Scaling solutions built on top of base blockchains (e.g., rollups, state channels) to improve speed and reduce costs.
- Payments: Protocols and platforms enabling crypto-based payments, remittances, or transaction infrastructure.
- Developer Tools: Toolkits, APIs, SDKs, and platforms that simplify blockchain application development.
- Gaming Studio: Companies or DAOs building blockchain-based games and metaverse experiences.
- Lending: DeFi protocols allowing users to borrow or lend digital assets, often with collateralization.
- Metaverse: Virtual environments with digital assets, NFTs, and immersive interactions often tied to Web3.
- AI Agents: Autonomous agents that can execute blockchain transactions or strategies without human intervention.
- Decentralized Application (dApp): Applications running on smart contracts, often user-facing (wallets, marketplaces, etc.).
- DePIN (Decentralized Physical Infrastructure Networks): Protocols that incentivize building and sharing physical infrastructure (e.g., wireless networks, sensors).
- DEX (Decentralized Exchange): On-chain platforms for peer-to-peer crypto trading without intermediaries.
- EVM (Ethereum Virtual Machine): Protocols and projects compatible with Ethereum's smart contract runtime.
- Governance: DAO and governance frameworks enabling token-holder voting and decentralized decision-making.
- Launchpad: Platforms hosting token sales (IDOs/IEOs), giving early access to projects.
- Marketplace: Platforms enabling the buying/selling of crypto goods, often NFTs or collectibles.

- Perpetuals: Exchanges or protocols offering perpetual futures contracts tied to crypto assets.
- Privacy: Protocols enhancing anonymity and confidentiality, such as mixers or zk-based systems.
- Stablecoin Protocol: Projects issuing or backing stablecoins pegged to fiat or commodities.
- Staking: Protocols where users lock tokens to secure a network and earn rewards.
- DAO (Decentralized Autonomous Organization): Member-governed organizations operating via smart contracts.
- RWA (Real World Assets): Protocols tokenizing traditional assets such as real estate, bonds, or commodities.
- Security: Cybersecurity, fraud detection, and protocol-audit services for crypto infrastructure.
- Trading Strategies: Quantitative and algorithmic trading platforms or protocols.
- Treasury Management: Tools for managing on-chain treasuries, often used by DAOs or crypto-native funds.
- zk-Proofs (ZKP): Cryptographic systems (zero-knowledge proofs) that enable privacy and scalability.
- API: Interfaces and middleware that connect Web3 protocols to apps and services.
- Bitcoin Scaling: Layer 2 or sidechain solutions for scaling Bitcoin (e.g., Lightning Network).
- Digital Identity: On-chain identity solutions (KYC, DID, verifiable credentials).
- E-commerce: Web3-enabled shopping platforms or payment systems.
- Internet of Things (IoT): Blockchain solutions applied to connected devices and sensor networks.
- Layer 1 (L1): Base-layer blockchains like Ethereum, Solana, or Avalanche.
- Mini App / Mobile: Mobile-first blockchain apps, mini-program ecosystems.
- Portfolio Management: Tools and dashboards for tracking digital asset portfolios.
- Restaking: Re-using staked assets (like ETH) to secure additional protocols.
- Smart Contract Platform: Blockchains optimized for running programmable smart contracts.
- Wallet: Software or hardware enabling custody and transactions of digital assets.

8.2.2 Focus Area Ranking by Retail ROI

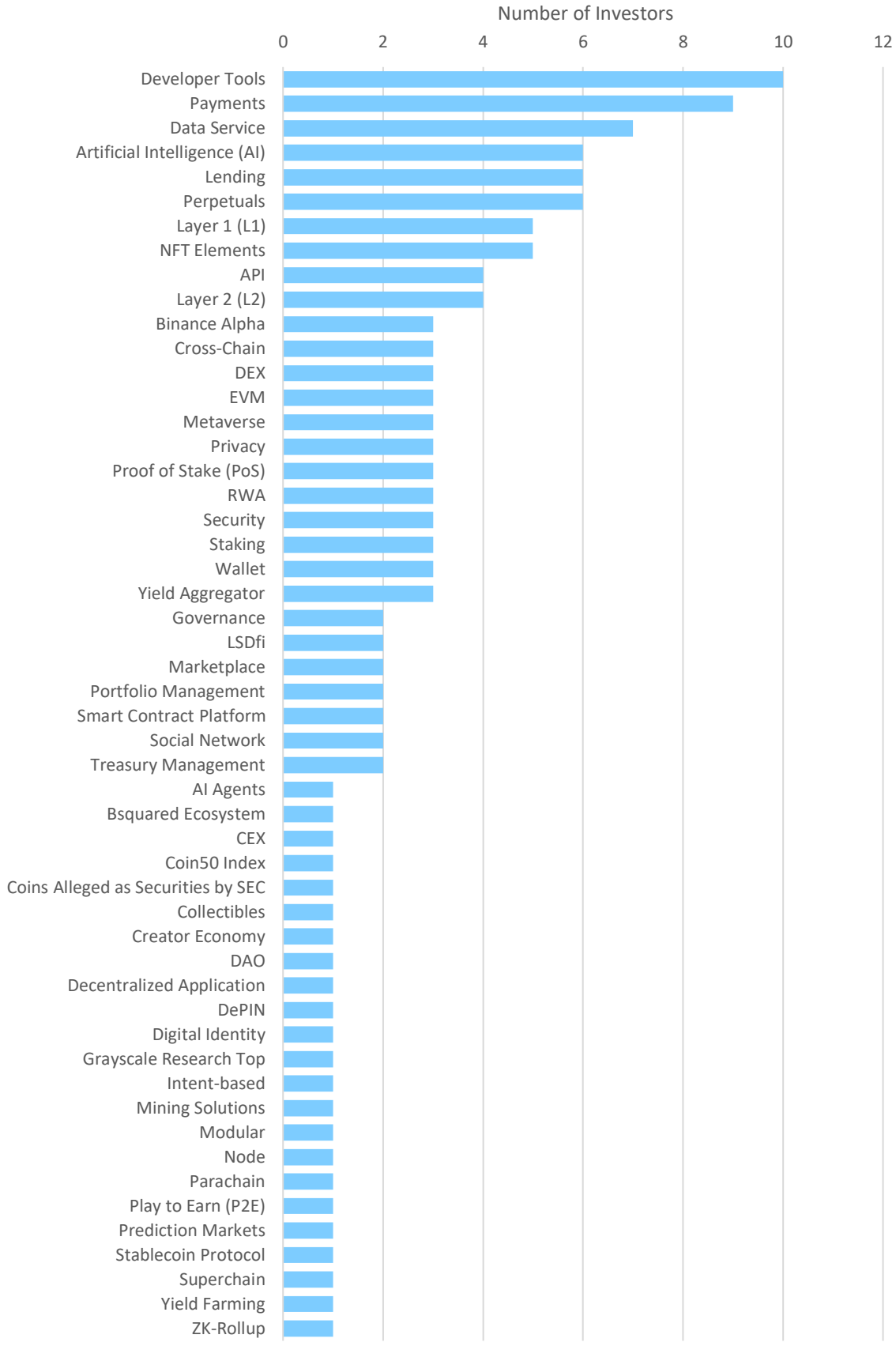

Figure 16. Focus Areas of the Top 20 VC Investors by Retail ROI. Updated the 8th September 2025. Source: CryptoRank.

When ranking by retail ROI, the most common themes are Developer Tools and Payments, with around half of the investors allocating to them. Data Services, AI, Lending, and Perpetuals also appear prominently, each attracting about a quarter of the top ROI-oriented funds. Interestingly, while categories such as NFT Elements and Gaming were central in the portfolio-size ranking, they drop into a secondary tier in the ROI-driven list. Instead, infrastructure-related segments like Layer 1, APIs, and Layer 2 gain visibility, highlighting a tilt toward foundational technologies rather than consumer-facing applications.

Key to focus areas:

- AI Agents: Autonomous, AI-powered entities capable of executing blockchain actions without human intervention.
- API: Interfaces that allow developers to connect applications to blockchain protocols and data.
- Binance Alpha: Early-stage or strategic projects incubated or supported by Binance.
- Bsquared Ecosystem: A niche blockchain ecosystem or project cluster, often specific to a fund's thematic focus.
- Collectibles: Digital items, often NFTs, with scarcity and tradable value.
- Coins Alleged as Securities by SEC: Projects flagged by regulators (notably the SEC) as potentially being securities.
- Coin50 Index: A benchmark or index tracking a basket of the top 50 coins.
- Cross-Chain: Infrastructure enabling asset and data movement across blockchains.
- Creator Economy: Platforms supporting creators through tokenized monetization, NFTs, or Web3-native tools.
- DAO (Decentralized Autonomous Organization): Community-governed organizations managed by smart contracts.
- Data Service: Oracles and analytics providers ensuring reliable blockchain data.
- Decentralized Application (dApp): End-user applications that run on smart contracts.
- DePIN (Decentralized Physical Infrastructure Networks): Incentivized networks for physical infrastructure like sensors or connectivity.
- DEX (Decentralized Exchange): Peer-to-peer crypto trading without intermediaries.
- Digital Identity: On-chain identity solutions (DIDs, verifiable credentials, KYC).
- Developer Tools: Toolkits, SDKs, and infrastructure to help build blockchain apps.
- EVM (Ethereum Virtual Machine): Ecosystem of protocols compatible with Ethereum's smart contract runtime.
- Governance: Protocols enabling token-based voting and decentralized decision-making.
- Grayscale Research Top: Focus areas highlighted by Grayscale's crypto research.
- Intent-based: Protocols enabling users to specify desired outcomes ("what") while the system determines execution ("how").
- Layer 1 (L1): Base blockchain networks like Ethereum or Solana.
- Layer 2 (L2): Scaling solutions operating on top of L1 blockchains.
- Lending: Platforms enabling borrowing and lending of digital assets.
- LSDfi: DeFi projects built on liquid staking derivatives.
- Marketplace: Platforms for buying and selling digital goods, often NFTs.
- Metaverse: Virtual worlds and immersive ecosystems powered by blockchain.
- Mining Solutions: Protocols and companies building technology for crypto mining.
- Modular: Architectures separating execution, settlement, and data availability layers.
- Node: Services/tools enabling blockchain node operation or access.
- Payments: Platforms facilitating crypto-based transactions and settlements.
- Perpetuals: Derivatives platforms offering perpetual futures contracts.

- Play to Earn (P2E): Games rewarding players with tokens or NFTs.
- Portfolio Management: Tools for tracking digital asset allocations.
- Prediction Markets: Platforms for speculating on outcomes using tokens.
- Privacy: Solutions that enhance anonymity and confidentiality of transactions.
- Proof of Stake (PoS): Consensus mechanisms where validators secure the network by staking assets.
- RWA (Real World Assets): Tokenized representations of traditional assets like real estate or bonds.
- Security: Cybersecurity and auditing services for blockchain.
- Smart Contract Platform: Blockchains specialized for programmable contracts.
- Social Network: Decentralized social media and community platforms.
- Stablecoin Protocol: Projects issuing or backing price-stable tokens.
- Staking: Locking tokens in a network to secure it and earn rewards.
- Superchain: Networks of interconnected blockchains that share security or functionality.
- Treasury Management: On-chain tools for managing reserves and DAO treasuries.
- Wallet: Software or hardware for digital asset custody and transactions.
- Yield Aggregator: Platforms that optimize returns by routing funds across multiple DeFi protocols.
- Yield Farming: DeFi strategies earning rewards by moving liquidity across protocols.
- ZK-Rollup: Layer 2 scaling solutions using zero-knowledge proofs for fast, cheap, secure transactions.

Glossary

Arbitrum (ARB)
Ethereum Layer-2 scaling solution governed by a DAO using the ARB token; faced governance controversy over treasury allocation.
Asset-Referenced Token (ART)
Stablecoin backed by a basket of assets (e.g., bonds, deposits), regulated under MiCA.
BCAP token
Blockchain Capital's security token representing ownership in their venture fund.
Bearer asset
Asset controlled entirely by whoever holds the private key (e.g., crypto tokens).
Bicameral governance
Dual-chamber model separating governance powers, e.g., Optimism's Token House (capital) and Citizens' House (public goods).
Binance
Leading crypto exchange and blockchain ecosystem, known for large funding rounds and token launches.
Blockdaemon
Crypto infrastructure company offering staking and node services, funded via equity without issuing a native token.
Blockchain
A distributed system that stores timeordered data in a continuously growing list of blocks. Each block contains information on transactions and business activities, and the entire network uses a consensus algorithm to reach an agreement on which block will be attached to the current recognized chain of blocks (Chen et al., 2021).
Bybit hack (2025)
$1.4B security breach on the Bybit exchange, driving attention toward custody and security investments.
Cap table
Record of a company's ownership structure, listing shareholders and stakes.
CASP (Crypto-Asset Service Provider)
Entity under MiCA providing services such as custody, exchange, trading, and wallet solutions.
Cliff (vesting)
Period during which no tokens/equity vest; after the cliff, vesting begins.
CoinSchedule
Data tracker for ICO statistics, widely cited in early token fundraising analyses.
Compound (COMP)
Lending protocol with strong quorum-based token governance, an early DeFi governance model.
Conviction voting
Voting system where influence increases with the time tokens are locked, rewarding long-term commitment.
Council governance
Governance led by a fixed group of institutions/enterprises with equal votes (e.g., Hedera Hashgraph).
Cryptocurrency
Digital money that uses cryptography to secure transactions and is built on decentralized networks, most often blockchains. It enables peer-to-peer value transfer without central intermediaries.
Cross-chain bridge
Infrastructure enabling tokens or data to move between blockchains; governance disputes often arise over provider choice.
Curve Wars

Competition among protocols to accumulate vote-escrowed CRV (veCRV) governance power to direct liquidity rewards.

Custody (crypto)

Secure storage of digital assets, often via regulated custodians (e.g., Fireblocks, Anchorage, BitGo).

DAO (Decentralized Autonomous Organization)

A blockchain-based system that enables people to coordinate and govern themselves mediated by a set of self-executing rules deployed on a public blockchain, and whose governance is decentralized and thus independent from central control (Hassan & De Filippi, 2021).

DAO treasury

Collective funds controlled by DAO token holders via governance proposals.

Delegation (governance)

Assigning voting power to another participant while retaining token ownership.

DeFi (Decentralized Finance)

Blockchain-based financial services (lending, trading, derivatives) operating without intermediaries.

Delegation transparency

Public tracking of how delegates vote, improving accountability.

dApps (Decentralized Applications)

Applications running on blockchain networks rather than centralized servers.

Digital signature

Cryptographic mechanism proving ownership of digital assets; foundation of early digital money systems.

Double-spending problem

Risk that a digital token could be spent twice; solved in Bitcoin via proof-of-work consensus.

Dual-token model

Governance system where one token captures economic value (staking/rewards) and another controls decision-making.

DYDX

Derivatives protocol that transitioned from centralized control to a DAO governed by the DYDX token.

E-Money Token (EMT)

Stablecoin pegged to a single fiat currency (e.g., euro, USD), regulated under MiCA.

ERC-20

Ethereum's standard for fungible tokens, enabling mass token creation during the ICO boom.

Equity-only deal

VC investment into company shares without token exposure.

Fireblocks

Digital asset custody and infrastructure firm, raised >$1.2B via equity, no token issuance.

Fork (blockchain)

A split in protocol code or governance that creates divergent versions of a blockchain.

FTT token

Exchange token issued by FTX, central to its balance sheet collapse.

FTX collapse (2022)

Bankruptcy of major exchange FTX due to misuse of customer funds and reliance on illiquid tokens.

Full-reserve requirement

Rule that stablecoin issuers must back tokens 1:1 with safe, liquid assets.

Governance capture

Disproportionate influence over protocol decisions by concentrated actors (e.g., VCs, whales).

Governance token

Token granting voting rights over protocol rules, treasury, and parameters (e.g., UNI, COMP, AAVE).

Governance by code

Hardcoding governance rules into smart contracts, minimizing human discretion (e.g., Stacks' Clarity contracts).

Hashgraph
Consensus mechanism used by Hedera, distinct from blockchain; fast, asynchronous Byzantine fault tolerant.
Hedera Hashgraph
Public distributed ledger governed by a global council of institutions instead of token-based voting.
Honest nodes (Bitcoin)
Nodes following protocol rules; Bitcoin's security depends on majority CPU power controlled by honest nodes.
Howey Test
U.S. legal test determining if an asset qualifies as a security based on investment contract criteria.
ICO (Initial Coin Offering)
Fundraising mechanism where tokens are sold to the public, often before network launch.
Illiquid token
Token with low trading volume, difficult to convert into cash without moving price.
LayerZero
Interoperability protocol; its association with VC interests created governance controversy in Uniswap.
Liquidity mining
Incentive program distributing tokens to users providing liquidity to a protocol.
Lockup (token)
Restriction preventing sale/transfer of tokens for a period.
MakerDAO (MKR)
Protocol where governance token holders control parameters like collateral and stability fees.
Meta-governance
Protocol or investor using governance tokens to influence decisions across other protocols.
MiCA (Markets in Crypto-Assets Regulation)
EU regulation providing a framework for crypto issuers, stablecoins, and service providers.
Mining (cloud mining)
Renting computational resources to mine cryptocurrencies; e.g., XY Miners raised $300M in 2025.
NFT (Non-Fungible Token)
Unique blockchain token representing digital/real-world assets; fractionalized collections may fall under MiCA.
Optimism governance
Bicameral DAO governance model with a Token House (economic) and Citizens' House (identity-based).
OTC (Over-the-Counter)
Direct token trade between parties, outside of public exchanges.
Plutocracy (token governance)
System where wealthy token holders dominate decisions.
Private key
Cryptographic key granting control over tokens; whoever holds it controls the funds.
Proof-of-work (PoW)
Consensus mechanism using computational puzzles; foundational to Bitcoin security.
SAFT (Simple Agreement for Future Tokens)
Investment contract giving rights to receive tokens once functional.
SAFE (Simple Agreement for Future Equity)
Founder-friendly contract giving rights to equity in a future round, often modified to include token side letters.
Security Council (DAO)
Multisig group with emergency veto/delay powers, e.g., Arbitrum DAO.

Security token
Blockchain token representing ownership in a regulated asset (e.g., fund shares, equity).
Self-referential token economy
Ecosystem relying on tokens it issues for reserves/liquidity, vulnerable to collapse (e.g., FTT).
Serum (SRM)
Token tied to FTX ecosystem, collapsed in 2022.
Side letter
Agreement granting investors extra rights (e.g., future tokens) alongside core contracts.
Smart contract
Digital contracts allowing terms contingent on decentralized consensus that are tamper-proof and typically self-enforcing through automated execution (Cong & He, 2019).
Soulbound token
Non-transferable token tied to an identity, often used for governance legitimacy.
Stablecoin
Cryptocurrency pegged to stable assets (e.g., USD, euro) to maintain price stability.
Sybil resistance
Methods (identity verification, attestations) to prevent fake accounts from gaming governance.
Timelock
Mandatory delay before proposals execute, used to safeguard governance.
Token velocity
Rate at which tokens circulate or are traded; often linked to speculation vs. utility.
Token warrant
Right to receive tokens in the future, often linked to equity rounds.
Tokenomics
Economic design of a token, covering issuance, supply, incentives, and governance role.
Treasury sale
DAO-approved sale of governance tokens to investors or partners.
UNI token (Uniswap)
Governance token used in Uniswap DAO to vote on proposals and treasury management.
Uniswap DAO
Protocol governance system using UNI tokens; subject of VC influence controversies.
Utility token
Token designed for use within a network (e.g., access, fees) rather than as an investment security.
Vesting schedule
Structured release of equity or token allocations over time to align incentives.
Vote-escrow model (veCRV, veBAL)
Lock tokens to gain voting power and yield boosts; voting power decays over time unless re-locked.
Whale dump
Large token sale by major holders, often triggering price crashes and community backlash.
Whitepaper
Foundational technical/investment document explaining a project, e.g., Bitcoin whitepaper.

Bibliography

Batiz-Benet, J., Santori, M., & Clayburgh, J. (2017). The SAFT project: Toward a compliant token sale framework. *SAFT Project White Paper, Cooley*.

Chen, L., Cong, L. W., & Xiao, Y. (2021). A brief introduction to blockchain economics. In *Information for efficient decision making: Big data, blockchain and relevance* (pp. 1-40).

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, *32*(5), 1754-1797.

Conlon, T., Corbet, S., & Hu, Y. (2023). The collapse of the FTX exchange: The end of cryptocurrency's age of innocence. *The British Accounting Review*, 101277.

CryptoRank (2025, July 16). *State of Venture Capital in Crypto, Q2 2025*. Retrieved 2025, September, from cryptorank.io: https://cryptorank.io/insights/reports/crypto-fundraising-report-Q2-25

Ellinger, E. W., Mini, T., Gregory, R. W., & Dietz, A. (2024). Decentralized autonomous organization (DAO): The case of MakerDAO. *Journal of Information Technology Teaching Cases*, *14*(2), 265-272.

Fenu, G., Marchesi, L., Marchesi, M., & Tonelli, R. (2018, March). The ICO phenomenon and its relationships with ethereum smart contract environment. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)* (pp. 26-32). IEEE.

Hallak, I. (2022). Markets in crypto-assets (MiCA). *European Parliament Research Service: London, UK*

Häring, W. & Wöckener, K. (2023, July 4). *MiCA Regulation: New regulatory framework for Crypto-Assets Issuers and Crypto-Asset Services Providers in the EEA*. Retrieved 2025, September, from whitecase.com: https://www.whitecase.com/insight-alert/mica-regulation-new-regulatory-framework-crypto-assets-issuers-and-crypto-asset

Hassan, S., & De Filippi, P. (2021). Decentralized autonomous organization.

Howell, Sabrina T., Niessner, M., & Yermack, D., Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales (June 2018). NBER Working Paper No. w24774, Available at SSRN: https://ssrn.com/abstract=3206449

Imtiaz, M. & Sabater, A. (2024, April 11). Global venture capital investment value, volume down in Q1 2024. Retrieved in 2025, September, from spglobal.com: https://www.spglobal.com/market-intelligence/en/news-insights/articles/2024/4/global-venture-capital-investment-value-volume-down-in-q1-2024-81180407

ING (2018, September). *Cryptocurrencies and tokens. ECB FXCG update.* Retrieved 2025, September, from www.ecb.europa.eu:
https://www.ecb.europa.eu/paym/groups/pdf/fxcg/2018/20180906/Item_2a_-_Cryptocurrencies_and_tokens.pdf

KPMG (2025, July). Venture Pulse Q2 2025. Retrieved in 2025, September from assets.kpmg.com: https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2025/07/kpmg-private-enterprise-quarterly-q2-25-global-report.pdf

Krause, D. (2025). The GENIUS Act: A New Era of US Stablecoin Regulation. *Available at SSRN 5127407*.

Nakamoto, S. (2008). Bitcoin whitepaper. *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, *9*, 15.

Thorn, A. (2025, July 31). Crypto and Blockchain Venture Capital – Q2 2025. Retrieved 2025, September, from galaxy.com: https://www.galaxy.com/insights/research/crypto-blockchain-venture-capital-q2-2025

U.S. Senate. (2025). *S.1582 — Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act of 2025*. 119th Congress. https://www.congress.gov/bill/119th-congress/senate-bill/1582/text

Xiao, L. (2025). The Adequacy of MiCA in Addressing Market Manipulation in the Crypto Asset Market.

Zetzsche, D. A., Annunziata, F., Arner, D. W., & Buckley, R. P. (2021). The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy. *Capital Markets Law Journal*, *16*(2), 203-225.