ETHERBRIDGE · RESEARCH

A FRAMEWORK FOR INVESTORS

The Crypto Weighing *Machine*

Everything you need to get off zero with cryptoassets. From Bitcoin to tokenisation, from networks to applications, and the investment lens that holds it all together.

Jason Carpenter

FOUNDER · ETHERBRIDGE

THE CRYPTO WEIGHING MACHINE

An Etherbridge publication.

Research and commentary by Jason Carpenter is published under the Chain Street brand on Substack. Etherbridge is a liquid long-only cryptoasset fund.

For more, visit **etherbridge.co** · **chainstreet.substack.com**

CONTENTS

What's Inside

INTRODUCTION

A Weighing Machine, Not a Voting Machine

> *“In the short run, the market is a voting machine, but in the long run, it is a weighing machine.”*
>
> — BENJAMIN GRAHAM

Benjamin Graham's observation is a useful frame for thinking about crypto today.

The asset class has spent its adolescence cycling through rampant speculation, wealth creation, and wealth destruction. Underneath all of that, something more structural has been taking shape.

Cryptoassets sit at the intersection of economics, computer science, and cryptography. Paul Tudor Jones puts it as plainly as anyone:

> *“Bitcoin is math, and math has been around for thousands of years. I like the idea of investing in something that is reliable, consistent, honest, and 100% certain.”*

Erik Voorhees makes the same point from a different angle:

> *“Code polices better than police. The laws of mathematics. The laws of code. These laws have meaning, they are powerful, they are consistent, they are worthy of respect.”*

Crypto extends well beyond Bitcoin. The tokenisation of currency and real-world assets is starting to rewire how financial markets settle, custody, and report. BlackRock's Larry Fink has been direct about where this leads:

> *“If you have a tokenised security, and you have a tokenised identity... the moment you buy or sell an instrument, it's known, it's on a general ledger that is all created together, you want to talk about issues around money laundering and all that, this eliminates all corruption, by having a tokenised system.”*

The growth numbers are hard to ignore. At the end of 2025, the global owner base reached 741-million, up from 659-million a year earlier and more than triple the base of five years ago. Bitcoin remains the dominant holding at 365-million owners. Ethereum grew the fastest over the year at 22.6%, reaching 175-million owners on the back of institutional treasury adoption and real-world asset tokenisation.

Younger generations continue to do the heavy lifting. The 25-34 age group remains the largest cohort of cryptoasset owners, with 35-44 close behind. As the baby boomer wealth transfer plays out over the next decade, asset allocation decisions will increasingly need to take this generational shift into account.

Fifteen years in, regulatory clarity is finally starting to crystallise. Investors need to understand the difference between crypto networks and crypto applications, and to think about this space in terms of innovation rather than speculation.

This is fundamentally an exercise in Schumpeter's creative destruction. Innovation is always undervalued at its inception. Investors who do the work to understand what is being built are positioned to capture the economic opportunity and, in doing so, shape what the financial system looks like next.

PART I

Bitcoin

Bitcoin sits at the centre of one of the most contested debates in modern finance. Its supporters see a technology that upgrades how we store and transfer value. Its critics see a volatile distraction or a speculative bubble.

The constituencies it has attracted tell you something about why it persists. Libertarians looking for a currency beyond government control. Forward-looking investors worried about the structural indebtedness of developed nation states. Technologists drawn to a new era of programmable money. People in countries with strict capital controls or high inflation who want a more stable monetary alternative.

This chapter walks through how Satoshi Nakamoto fused existing breakthroughs in cryptography, distributed systems, and consensus mechanisms to build the first working decentralised digital currency. It explains why many call Bitcoin "digital gold" and what makes it interesting from an investment perspective.

Satoshi's Breakthrough

Bitcoin was not the first attempt at digital money. David Chaum's DigiCash, Wei Dai's b-money, and Nick Szabo's Bit Gold all came before it, introducing concepts like blind signatures, cryptographic hashes, and distributed architectures.

None of these projects cracked the core problem. A decentralised digital cash that could prevent the same coin from being spent more than once, without a central coordinating entity.

The double-spend problem

The double-spend problem arises whenever something of value is represented by a digital file. Files can be copied. In most digital interactions this is the norm. When you send an email or a photo, you are actually sending a copy and keeping the original. For money, the ability to copy at will would destroy the value of the asset.

The traditional fix was to introduce a central authority. A bank or payment processor tracks balances and settles transactions. If you try to spend the same $100 twice, the intermediary blocks the second attempt. This works in practice but introduces a single point of failure and control. The system depends on the intermediary staying online, staying honest, and acting in the user's interest.

Satoshi's breakthrough was replacing the trusted intermediary with a network consensus mechanism. Bitcoin solved the double-spend problem without banks, payment processors, or any central authority. A global network of participants, each running the same open-source software, coordinates to agree on one shared ledger of valid transactions.

Proof of work, conceptually

Proof of work is the process by which the Bitcoin network forces participating computers (nodes) to perform a certain amount of computational effort before a new batch of transactions (a block) can be accepted as valid.

The design does three things at once.

Effort is expended. Any would-be attacker needs to devote significant computing resources and energy to alter past transactions.

Security is decentralised. Anyone can join the network and try to produce blocks, so control is spread rather than concentrated.

Incentives are aligned. Network participants (miners) are rewarded with newly minted bitcoins and transaction fees for performing the work honestly, tying the system's security to real-world economic incentives.

Proof of work makes manipulating the ledger expensive and verifying its integrity cheap. That asymmetry is the heart of how a leaderless financial network stays secure.

Proof of work in more detail

Proof of work involves repeatedly hashing (applying a cryptographic one-way function to) a block header until the resulting hash meets a network-defined difficulty target. Each hashing attempt is like buying a lottery ticket. Find a winning ticket and the miner publishes the block and earns the reward.

Even a minor change to a block, like altering a single transaction, produces a completely different hash. Resubmitting a modified block requires redoing all previous computational effort. To reverse multiple past transactions, an attacker would need to re-mine all affected blocks and simultaneously outpace the current network. That demands immense computing resources and energy, and is prohibitively expensive unless the attacker controls a majority of the network's total computing power.

Confidence in Bitcoin's functionality

Bitcoin's security rests on cryptographic hashes and on robust economic incentives. Miners invest real resources, electricity and specialised hardware, to find proof-of-work solutions. Honest miners earn newly minted bitcoins and transaction fees when they add valid blocks. Any attempt at fraud requires enormous resources, yields no reward, and is rejected by the network.

Participants have a stronger economic incentive to follow the rules than to break them. Cryptographic security, distributed consensus, and financial incentives reinforce each other, and that is what gives Bitcoin its resilience.

What Makes Bitcoin Interesting from an Investment Perspective

Apolitical and resistant to control

Bitcoin is not governed by any single person, corporation, or government. The underlying software is open-source. Anyone can participate by running a node or mining. No central authority can unilaterally seize or censor transactions or change the rules.

This apolitical structure appeals to a wide range of people. Libertarians seeking a currency unbound by government control. Citizens in authoritarian regimes who worry about currency devaluations or asset seizures. Anyone whose trust in the existing financial architecture has eroded.

The point becomes sharper when viewed through the lens of global finance. Traditional financial transactions and asset custody rely on institutions and intermediaries that are subject to political influence, regulatory capture, or regional instability. Bitcoin functions as a neutral settlement layer. Some have called it a platform for enemies. Parties who do not trust each other, or who are separated by geopolitical tensions, can still transact securely and transparently through the Bitcoin network.

The ledger is publicly verifiable and cannot be tampered with by any single actor. That enables a level of financial cooperation and coordination that is difficult to achieve in politically charged or adversarial environments. The neutrality gives Bitcoin real utility in cross-border trade, international remittances, and financial infrastructure in conflict zones or unbanked regions.

The difficulty adjustment

Bitcoin's difficulty adjustment is the mechanism that automatically regulates how hard it is to mine new blocks. The protocol recalibrates the target hash difficulty approximately every 2,016 blocks (about every two weeks), aiming to keep the average time between new blocks at around 10 minutes. If more miners join and blocks are found too quickly, the difficulty rises. If miners drop off and blocks slow down, the difficulty falls.

This was one of Satoshi's most brilliant insights. By tying block creation to a dynamic difficulty parameter, the Bitcoin network ensures a fixed, predictable, non-discretionary issuance rate. No matter how many miners participate, no more than the protocol's programmed supply of 21-million bitcoins can ever be created. The result is a digital asset with monetary characteristics that are fundamentally different from fiat currencies, whose supply can be influenced by central banks and policy decisions.

Chancellor on the brink of another bank bailout

When Satoshi mined the first Bitcoin block, the "genesis block", the embedded headline read: *Chancellor on brink of second bailout for banks*. It served as both a timestamp and a nod to the context Bitcoin was born into, the aftermath of the 2008 global financial crisis.

In the years since, governments worldwide have adopted highly accommodative monetary policies. Global debt has reached unprecedented levels and concerns about currency debasement have followed. Rising debt-to-GDP ratios in developed economies have prompted some investors to question the long-term stability of the world reserve currency and the broader international financial system.

Bitcoin has emerged as a perceived hedge. A release valve for those sceptical of central banks' capacity to maintain monetary discipline. The belief is that because Bitcoin's supply schedule cannot be changed to accommodate new credit cycles or political agendas, it offers a form of digital gold. Scarce, portable, and not easily manipulated. That promise continues to draw interest from individuals, institutions, and even nation states searching for a hedge against currency devaluation or systemic financial risk.

Inelasticity in an elastic world

Bitcoin is a provocation in a world defined by supply elasticity. Fiat currency's defining feature is the ability to extend supply to meet demand. This same mechanism socialises losses across all holders and erodes the purchasing power of those who store their wealth in local currencies.

Commodities respond to price too, though less uniformly. Precious metals like gold are relatively inelastic compared to industrial commodities like oil or copper, but even gold responds eventually. A sustained price increase makes previously uneconomic mining ventures viable, draws fresh supply onto the market, and dampens the rally.

Bitcoin breaks this pattern entirely. Higher prices attract more miners, but the difficulty adjustment absorbs the extra effort. Issuance cannot accelerate. No amount of future demand can lift supply above its predetermined schedule. The supply curve is vertical, which means demand can only express itself through price. In a financial system built around elastic responses, this is what makes Bitcoin interesting.

PART II

Beyond Bitcoin

The word *blockchain* never appears in the original Bitcoin white paper, yet the network Satoshi Nakamoto launched quietly introduced one of the most important ideas in modern computing. A decentralised, leaderless system can coordinate people and value at a global scale.

Bitcoin's brilliance is its simplicity. An elegant, purpose-built protocol for secure, censorship-resistant transactions. That same simplicity also limits its flexibility. Bitcoin was not designed to handle more complex logic or dynamic interactions beyond basic transfers of value.

Bitcoin sparked a wave of imagination. Developers, entrepreneurs, and technologists looked at its foundational ideas and asked a bigger question. What if this model of trustless coordination could be extended beyond money?

They envisioned blockchain networks that were more expressive, programmable, and adaptable. Networks capable of addressing deeper problems in our financial infrastructure and internet architecture. An explosion of experimentation followed, with new systems exploring different trade-offs between scalability, decentralisation, and security.

This section walks through what these dreamers believe is broken in the current system, what they are building in response, and why it might matter for the future of finance and beyond.

The Problem, A Fragmented Internet and Financial System

The internet transmits information between computers seamlessly. It does not inherently track who owns what or how much of it they own. This gap, the same double-spend problem we discussed earlier, forces us to trust intermediaries with our financial records. Banks, payment processors, and brokerages maintain proprietary databases. Each stores ownership details in a siloed environment. The setup delivers a familiar user experience and at the same time fragments our networks and restricts the fluid movement of money and data.

The first issue is siloed, permissioned servers. Each financial institution runs its own system, rarely designed to interface smoothly with others. Transactions pass through multiple parties, picking up paperwork, fees, and friction along the way. Users have to manage accounts across platforms. Entrepreneurs have to build products that integrate neatly into a tapestry of disparate technologies.

Fragmentation also drives high transaction costs. Whether you are moving money internationally or domestically, the payment process involves multiple intermediaries, each adding overhead. Service fees accumulate and get passed through to consumers and businesses. Over time these expenses become significant barriers to the free flow of capital, particularly for smaller enterprises and individuals.

High barriers to entry stifle innovation in financial services. New entrants need to navigate intricate regulatory frameworks and build partnerships with incumbent institutions before they can offer even basic payment or banking solutions. The environment favours large, well-capitalised firms and discourages smaller, more agile ventures from bringing fresh ideas to market.

Legacy arrangements also foster local banking oligopolies, especially in smaller economies. Large banks act as gatekeepers, wielding control over the financial infrastructure and limiting both competition and customer choice. Their dominance lets them maintain high net interest margins, the difference between lending and deposit rates. In many emerging markets this translates into extractive net interest margins of 5–10%. The costs increase the global cost of capital, reduce access to affordable credit, and dampen entrepreneurship, homebuilding, and economic growth.

Because established institutions control the primary channels of finance and profit handsomely from them, they have few incentives to experiment or evolve. Potential disruptors struggle to gain a foothold. Established firms focus on preserving the status quo rather than developing new solutions.

Fragmentation, high costs, barriers to entry, entrenched gatekeepers, and limited innovation. Together these highlight the need for a system that can unify and democratise financial services rather than relegating them to siloed databases.

Some might argue that fintech has already brought significant innovation to finance. Fintech largely operates on the surface of legacy infrastructure. The companies build sleek interfaces and user experiences while remaining tethered to the same fragmented backend systems they aim to improve. They often add new layers of complexity rather than simplifying the core.

Real innovation does not dress up old systems. It rethinks them. Blockchain and smart contract platforms take a fundamentally different approach, rebuilding financial coordination from the centre outward with open, programmable, and unified systems designed for a digital world.

The Solution, A New Internet and Financial System

Public blockchains take a different approach to managing financial data and transactions. Instead of relying on siloed, permissioned servers, these networks spread responsibility across a global, permissionless set of nodes. A public blockchain functions as a unified server. A single, standardised infrastructure that anyone can use to send, receive, and store value. This eliminates many of the inefficiencies that arise when banks and payment platforms operate their own proprietary, largely incompatible systems. Trust no longer hinges on an institution's brand or reputation. It comes from open-source software and decentralised consensus.

Blockchains also host smart contracts. Pieces of code that automatically execute certain actions when specified conditions are met. Like a digital vending machine, a smart contract removes the need for intermediaries to coordinate or approve a process, which dramatically lowers operational costs. The automation opens the door to an entirely new realm of financial product design, from decentralised exchanges to automated insurance claims, all while reducing human error and manual overhead.

Blockchains enable the free flow of capital across borders, a stark contrast to the cumbersome and expensive processes of SWIFT, ACH, or local banking channels. Anyone with an internet connection can bypass the gatekeepers who typically impose restrictions, fees, and delays on international transfers. This frictionless movement of funds benefits individual users and small businesses, and it weakens the stranglehold of local banking oligopolies by offering a global alternative that drives competition and innovation.

Smart contracts also enable widespread automation. Tasks traditionally performed by large operations teams can be handled by a handful of engineers overseeing automated protocols. A small company can manage billions of US dollars in assets through well-designed on-chain applications. Reducing reliance on manual processing and human intervention lowers costs and scales more efficiently.

Public blockchains also present lower barriers to entry. Instead of seeking permission from established financial institutions, startups and developers can tap into a permissionless system where anyone can build, deploy, or interact with decentralised applications. This encourages open competition and brings new ideas and solutions into the market without the gatekeeping structures that characterise traditional finance. Over time the benefits of a truly global, unified financial infrastructure could ripple through economies worldwide, spurring innovation, broadening financial access, and reshaping how we think about money and markets.

Why open-source?

Open-source development is the cornerstone of this new financial architecture. By making code publicly available and freely accessible, open-source projects invite scrutiny and collaboration from a global pool of developers.

The transparency leads to more secure and robust systems. The cliché is that "many eyeballs tame complexity." With enough attention and participation, bugs are spotted faster, vulnerabilities are patched more effectively, and improvements are proposed and implemented in real time. The result is software that is more reliable, more secure, and more resilient than what any single team could achieve behind closed doors.

Open-source also dramatically reduces development costs. Developers can build on existing frameworks, tools, and protocols, standing on the shoulders of giants. The modular, composable approach accelerates iteration and enables rapid innovation. New financial applications can be created, tested, and deployed at a fraction of the cost and time it would take inside traditional institutions. The open-source ethos empowers individual builders and fosters a culture of permissionless experimentation, where ideas rise or fall on their own merit, not on the gatekeeping of incumbents.

A network built in the open for anyone to use, improve, or build upon. Inclusive, adaptable, and trustworthy.

Smart contract basics

Smart contracts are self-executing pieces of code that run on a blockchain. They tie agreements directly to enforcement and remove the need for manual oversight or trusted intermediaries.

When predefined conditions are met, the contract carries out the agreed-upon actions automatically. Transferring funds, issuing tokens, or updating records. The automation reduces ambiguity, delays, and the risk of non-compliance, which makes smart contracts especially useful for financial services where precision and reliability matter.

What makes smart contracts powerful is their ability to make assets programmable. Instead of static ownership and manual processes, financial products can respond to real-time inputs and evolve based on logic encoded directly into the contract. Loans, insurance policies, swaps, and entire exchanges can be represented as on-chain applications.

Much of finance can be distilled into smart contracts. Compact, transparent programs that enforce rules and move value with minimal overhead. They are the foundation for a more dynamic, automated, and accessible financial system.

The Potential Benefits

Public blockchains are a major technological upgrade to existing financial and internet infrastructure. Replacing fragmented, siloed systems with unified, permissionless networks promises a step-change in efficiency, transparency, and scalability. Financial institutions stand to benefit enormously. They will be able to automate more with fewer resources, reduce reliance on costly intermediaries, and offer smarter, more adaptive products.

What cloud computing did for IT, blockchain may do for finance. It streamlines operations, expands reach, and dramatically lowers costs.

This new infrastructure makes finance more expressive. It enables the creation of entirely new financial instruments and markets while enhancing the durability and portability of existing ones. Smart contracts let institutions encode complex terms directly into programmable money, opening the door to more dynamic, real-time financial services. For banks, asset managers, and fintechs, the opportunity is significant. A more open, automated, and composable financial system unlocks a wave of innovation and productivity that could reshape how money moves and how markets function across the globe.

PART III

Tokenisation

Tokenisation is the process of representing the value of any asset, tangible or intangible, as a token on a blockchain. Think of these tokens as digital wrappers that hold the essential information about the underlying asset. A share of stock, a US Treasury bill, a mutual fund, or a physical commodity like gold. By placing assets on a public, permissionless ledger, tokenisation brings new levels of efficiency, transparency, and accessibility to finance.

When an asset is tokenised, it is wrapped in a uniform digital container. This standardised approach allows for easier transfer, fractional ownership, and instant settlement while reducing paperwork and intermediary costs. Tokenised assets are also interoperable with smart contracts. Pieces of code that can automate tasks like distributing dividends or enforcing regulatory constraints.

A good example of tokenisation working in a regulated context is ERC-3643, a specific Ethereum token standard designed for security tokens. Assets that fall under existing securities laws. ERC-3643 helps issuers and investors meet compliance requirements while still benefiting from blockchain's openness and programmability.

Some of its key features include the following.

- **Compliance management.** Tokens embed compliance logic directly in their smart contract code, ensuring they adhere to regulations across multiple jurisdictions.
- **Investor whitelisting.** Transfers of these tokens are restricted to verified and compliant investors, which prevents unauthorised purchases or sales.

- **Interoperability.** Because ERC-3643 builds on the broader Ethereum ecosystem, these tokens can interact seamlessly with decentralised finance (DeFi) platforms, exchanges, and other Ethereum-based applications.
- **Programmable controls.** Smart contracts can automate tasks like paying dividends, executing corporate actions, or managing investor data without manual intervention, which dramatically reduces administrative overhead.

By putting assets on a common protocol and making them programmable, tokenisation unlocks enormous latent potential. Instead of relying on manual processes, everything from shareholder voting to coupon payments can be automated through code. Standardising hundreds of thousands and potentially millions of different securities under the same token interface means that any tokenised asset can interact with any other application or smart contract on that blockchain.

The interoperability is a game-changer. In a traditional setting, each asset class often runs on its own bespoke systems, requiring complicated integrations and significant administrative work. Once an asset is tokenised under a widely adopted standard like ERC-3643, its "compatibility mode" with DeFi, digital wallets, and trading venues is already baked in. The result is a vast simplification of processes and a broadening of market access. Whether streamlining corporate actions or enabling real-time settlement across global exchanges, tokenisation promises to create a more efficient, inclusive, and dynamic financial ecosystem.

Stablecoins

The "killer app" for blockchain technology so far is not a revolutionary reinvention of finance. It is the US Dollar stablecoin. By design, a stablecoin maintains a 1:1 peg with a traditional currency (often the Dollar), combining the trust and

familiarity of fiat money with the borderless efficiency of the blockchain. Unlike more volatile cryptocurrencies, stablecoins aim to preserve the stable purchasing power of the underlying currency, which makes them well-suited for everyday transactions and global commerce.

There are four main varieties of on-chain Dollars worth understanding.

Fiat-backed stablecoins

Fiat-backed stablecoins include coins like Circle's USDC and Tether's USDT. Each token corresponds to an actual US Dollar (or a cash equivalent) held in a custodial account. In principle, token holders can redeem their stablecoins for Dollars through the issuing company. These coins bring digital convenience to traditional currency and require trusting the issuer to hold adequate reserves and operate transparently.

Crypto-collateralised stablecoins

Crypto-collateralised stablecoins like Sky's (formerly MakerDAO) USDS use cryptoassets like Ethereum's ETH and tokenised US Treasuries as collateral. Users lock these assets in an on-chain smart contract, which mints new stablecoins in return.

Because the collateral can be volatile, these systems over-collateralise to ensure they can absorb market swings and maintain the peg. The result is a more decentralised framework. There is no central authority holding the collateral, and algorithmic rules drive liquidation or issuance as needed.

Derivative-based stablecoins

A newer approach is seen with derivative-based stablecoins like Ethena's USDe. Instead of holding a simple pool of collateral, they use a delta-neutral strategy to balance long and short positions in assets, effectively hedging against volatility. The design can reduce the burden of managing large collateral reserves while still aiming for a stable Dollar value. It introduces complexity. Robust on-chain derivative markets and careful protocol design are needed to manage liquidity and market risk.

Deposit tokens

A fourth category has emerged directly from the banking system. Deposit tokens are blockchain representations of commercial bank deposits, issued by the bank that holds them. JPMorgan's JPMD, which launched on Coinbase's Base network in late 2025, is the first major example on a public blockchain. Unlike a fiat-backed stablecoin, a deposit token is not a claim on a segregated reserve of cash and Treasuries. It is a direct claim on the issuing bank. Sitting inside the fractional reserve system and carrying the same regulatory and insurance protections as a traditional deposit.

The structure has two important consequences. First, deposit tokens can pay interest to holders, because the underlying deposit itself earns yield within the bank's balance sheet. Fiat-backed stablecoins typically cannot, since the issuer keeps the yield from reserves. Second, they address a structural problem banks face with conventional stablecoins. For every Dollar a client converts into a stablecoin, a bank potentially loses multiple Dollars of deposit-funded lending capacity. Deposit tokens let banks participate in on-chain settlement without cannibalising their own balance sheets. Expect most major banks to follow JPMorgan's lead over

the coming years, with deposit tokens becoming the preferred on-chain Dollar for institutional flows while fiat-backed stablecoins continue to dominate retail and cross-border use.

Stablecoins open the door to remarkable possibilities that go beyond simply digitising the Dollar. They can dramatically improve cross-border payments, reducing the cost and friction typically associated with sending remittances or settling international invoices. In decentralised finance (DeFi), stablecoins serve as a reliable medium of exchange. They reduce the volatility of more speculative cryptoassets and enable more advanced services like automated lending, derivatives, and yield strategies.

Stablecoins also enhance financial inclusion, especially in emerging markets with limited banking infrastructure or local currencies prone to rapid devaluation. With just a mobile phone, individuals can store and transact in digital Dollars, which can stabilise their savings and unlock new avenues for trade. Thanks to near-instant settlement and sub-cent transaction fees, stablecoins are well suited to micropayments. This paves the way for streaming services where users pay for every minute of content viewed, and pay-as-you-go models in software development and open-source collaboration.

What makes stablecoins different to existing payment systems

It is tempting to think of stablecoins as a digital upgrade to existing payment rails. A faster or cheaper version of what banks and card networks already do. That framing misses what they actually are. Stablecoins are structural departures that, taken together, create a payments category that did not previously exist.

Six properties in particular set them apart.

- **Self-custody without an intermediary.** A stablecoin like USDT can be held directly in a blockchain wallet, with no requirement to maintain a relationship with a bank, payment processor, or any other financial institution. The peg is not maintained by the issuer's goodwill toward any individual holder. It is maintained by arbitrage mechanics. If USDT trades below $1, arbitrageurs redeem tokens at par, supply contracts, and the peg is restored. The user holds an asset whose value is defended by the structure of the market itself.

- **Push payments with final settlement.** Stablecoin payments are push transactions. The payer initiates, the funds arrive, and the transaction is final at the moment of broadcast. This is fundamentally different from credit card transactions, which are pull transactions carrying chargeback risk, or ACH, which settles in batches across several days. The closest analogue in traditional finance is a wire transfer, except stablecoin payments are available to anyone, around the clock, without a banker's involvement.

- **Permissionless access.** Anyone who is not on a sanctions list can create a blockchain wallet and begin sending or receiving stablecoins without asking permission from any intermediary. There is no onboarding process, no application, no approval. The network has no concept of a relationship with the user. It simply processes transactions. This is a profound departure from traditional finance, where access to basic payment services is gated by institutional willingness to serve a given customer, jurisdiction, or use case.

- **Open rails with low overhead.** Building a financial product on stablecoin rails does not require permission from legacy financial infrastructure. There are no correspondent bank agreements to negotiate, no SWIFT membership to acquire, no card scheme licence to obtain. What it does require is compliance with local regulatory frameworks and the engineering capability to build. The cost implications are structural. A neobank built on stablecoin rails might cost under a million dollars in engineering talent to launch, compared to hundreds

of millions for a bank charter or tens of millions for a cross-border money transmitter licence. The barrier to entry is no longer capital. It is capability.

- **Programmable and interoperable by default.** Stablecoins are not captive to any single database administered by a bank, government, or consortium. Developers can write smart contracts that interact with them directly, without permission, building financial products whose logic is conditional on the settlement of other on-chain transactions. This is genuine interoperability, and it stands in sharp contrast to the walled-garden architecture of SWIFT, Visa, and ACH. Each of those is a closed network with its own gatekeeping.
- **Continuous settlement.** Stablecoins settle during the roughly 76% of hours in any given week when banks are closed. They settle on Christmas Day, on New Year's Day, and on public holidays. They settle at three in the morning on a Sunday in Johannesburg, to a counterparty in Harare. The correspondent banking system, which routes the majority of cross-border Dollar payments through New York, operates within business hours and within New York's time zone. The contrast matters most for anyone who lives or works outside those constraints, which is to say most of the world.

These six properties do not simply make stablecoins better. They make them different in kind. Any analysis of their long-term role in the financial system needs to start from that recognition.

Failed experiments in stablecoins

The potential for stablecoins is enormous and the path forward has been paved with significant experimentation. Not all of it has succeeded. Algorithmic stablecoins, in particular, have attracted both excitement and controversy. Some projects have even explored CPI-linked stablecoins, designed to preserve purchasing power

rather than simply maintain a 1:1 peg to the US Dollar. Many view this as a promising innovation that could offer a more stable long-term store of value, especially in inflation-prone environments.

These experiments carry real technical and economic risks. The collapse of Terra's UST in 2022 is a stark reminder. UST relied on a reflexive mechanism involving its native network token, LUNA, where the value of UST was intertwined with speculative demand for the collateral asset, LUNA. When confidence faltered, the entire system unravelled in a self-reinforcing death spiral, wiping out billions of Dollars and damaging trust across the ecosystem. As the stablecoin space continues to evolve, investors, users, and developers need to remain vigilant. Innovation brings opportunity, and it also brings significant risk.

The state of stablecoins

Today, stablecoins are one of the most widely adopted applications of blockchain technology. The combined market capitalisation is just over USD318-billion at the start of 2026. The total has grown more than fivefold in under four years and now rivals the balance sheets of mid-sized commercial banks. Tether's USDT continues to dominate the landscape, accounting for approximately 61% of all stablecoins in circulation at a market cap of around USD187-billion. Circle's USDC remains the second-largest issuer at roughly USD75-billion, or about 25% of the market. The remainder is split among a growing cohort of challengers, with Ethena's synthetic USDe having emerged as the most notable new entrant and crossing USD14-billion in supply.

On the infrastructure side, the Ethereum ecosystem, including its layer two networks, hosts well over 60% of total stablecoin supply and remains the dominant settlement environment, attracting the bulk of institutional flows, tokenisation activity, and real-world asset issuance. Tron sits firmly in second place at around 25% of supply, having consolidated its role as the global remittance rail thanks to

low fees and deep penetration in emerging markets. Solana has emerged as a credible third, now one of the top three chains for stablecoin supply and increasingly used for high-throughput payments. The remainder is distributed across BNB Chain and other smart contract platforms, each carving out roles based on their particular trade-offs in scalability, cost, and ecosystem depth. Deposit tokens, discussed above, are tracked separately from the stablecoin market and remain a small but rapidly growing category.

Are stablecoins money for machines?

The rise of blockchain is unfolding alongside another transformative force, artificial intelligence (AI). As AI systems grow more autonomous and capable of making decisions, transacting, and interacting with the world on behalf of users or organisations, a compelling question emerges. What financial system will they use?

It is hard to imagine AI agents relying on today's fragmented, permissioned infrastructure. The legacy financial system, with its manual processes, jurisdictional silos, and unpredictable settlement times, is simply not designed for autonomous, real-time economic activity. Stablecoins on public blockchains offer a natural fit. Global, permissionless, programmable money that AI agents can send, receive, and manage without human intervention.

An AI agent could provide services, earn stablecoins from a global audience, and reinvest those earnings by buying more compute power, training data, or even the services of other AI agents. In this vision of the future, stablecoins may become the native currency of machine economies, enabling new forms of economic coordination that are as fluid and autonomous as the agents themselves.

This is no longer a purely theoretical picture. The infrastructure to support it has come together with surprising speed. In August 2025, a group of engineers from the Ethereum Foundation, MetaMask, Google, and Coinbase co-authored ERC-8004, the Trustless Agents standard. It gives every AI agent a persistent on-

chain identity, a verifiable reputation that accumulates across tasks, and a standardised way to discover and transact with other agents. A complementary payment protocol called x402 allows agents to settle for services autonomously using stablecoins, with pricing and authorisation embedded directly in the transaction flow.

ERC-8004 launched on Ethereum mainnet at the end of January 2026. The growth since has been remarkable. The Ethereum ecosystem now hosts over 101,000 registered agent services, up from essentially zero at the start of the year. These are autonomous software entities with wallets, reputations, and the ability to pay and be paid, deployed and operating entirely on-chain.

The machine economy is not arriving at some distant point on the horizon. It is arriving now. Stablecoins, combined with agent identity and payment standards, are becoming the default settlement layer for a rapidly emerging class of economic actors that did not meaningfully exist a year ago. For anyone thinking about the long-term role of on-chain Dollars in the financial system, this is the most under-appreciated data point on the board.

Real World Assets

With the foundations of tokenisation now clear, it is easier to see how stablecoins represent just the tip of the iceberg. Stablecoins have successfully shown how a traditional asset can be wrapped and placed on a blockchain by packaging US Dollars into a digital token. Beyond currencies, almost any asset can take on this new digital form. Bonds, real estate, private credit funds, equities, commodities, and more. The idea is simple. If you can define and enforce ownership rights through smart contracts, you can bring real-world value onto a global, permissionless network.

The shift from theoretical possibility to measurable reality has happened quickly. Tokenised funds, the category that includes on-chain US Treasuries and money market funds, have grown from around USD1.08-billion at the end of 2021 to over USD20.5-billion today. Tokenised commodities, dominated by gold-backed tokens like Tether Gold and Paxos Gold, have climbed from roughly USD536-million to around USD5-billion over the same period. Tokenised equities, which barely existed in 2021, now sit at over USD525-million, having grown through 2025 as platforms like Robinhood, Kraken, and Backed extended access to US stocks and ETFs to non-US investors on public blockchains. Private credit, corporate bonds, and real estate are all following the same trajectory. The absolute numbers are still small relative to the conventional markets they track, and the growth rates are telling. A category worth a few billion Dollars five years ago is approaching USD30-billion today, and institutional capital is only starting to arrive.

The composition of this growth reveals something important about which assets move on-chain first. Capital is flowing into instruments that fit within existing institutional workflows. Government securities, money market funds, gold, and private credit. Not exotic use cases. BlackRock's BUIDL, Franklin Templeton's BENJI, Circle's USYC, and Ondo's suite of products have each attracted billions in assets under management, validating the model for regulated asset managers. The SEC, NYSE, and Nasdaq have all moved into this space during 2026, with live tokenised money market funds now settling trades intraday and major exchanges building 24/7 tokenised securities infrastructure. What started as a crypto-native experiment has become a traditional finance priority.

The implications of this shift are enormous. By turning real-world assets into digital tokens, markets can become more transparent, liquid, and programmatically interoperable. A tokenised bond or fund can plug directly into decentralised exchanges, lending platforms, and automated portfolio management tools, lowering friction and opening new opportunities for yield generation. Settlement that once took days can occur in seconds. Middlemen that once added cost and complexity

can be replaced or streamlined by code. Tokenisation is an upgrade to financial market infrastructure that can bring efficiency gains and new creative possibilities for nearly every asset class.

Beyond immediate cost and speed benefits, programmability is the greatest superpower of tokenised assets. Transactions can be automated according to custom rules. Distributing dividends, managing fractional ownership, splitting royalties. The rules of engagement, built into smart contracts, enforce themselves without manual intervention. Because all tokenised assets operate on a shared protocol (or at least on blockchains that can interoperate via bridges), each token can integrate with a global ecosystem of decentralised applications.

The trajectory is clear. Tokenised real-world assets are no longer a speculative thesis. They are an emerging reality, and the line between traditional and on-chain finance is dissolving faster than most observers expected.

Blockchains are Starved for Quality Productive Assets

Finance plays a vital role in capitalism. It channels capital into promising ventures, brings future growth into the present, and helps accelerate economic progress. Finance on its own is not an end. Without productive assets like startups, businesses, infrastructure, and governments, finance quickly becomes a closed loop. Value stops being created and starts being shuffled. Speculation replaces utility, and the system devolves into a zero-sum game driven by hype and short-term gains.

Bitcoin introduced a seismic shift in how we think about money, offering a non-sovereign digital store of value in an increasingly fractured world. Stablecoins followed, refining how Dollars move in the internet age and giving billions access

to cheap, stable, and borderless money. Both are transformative. Beyond these foundational pillars, much of the cryptoeconomy still struggles to prove its broader utility. DeFi protocols have matured and some generate meaningful revenues, but the ecosystem remains largely speculative. It cycles through narratives, tokens, and trends with limited connection to the real world.

This speculative character is not incidental. It reflects something structural about where value has come from in crypto until now. Historically, the value of cryptoassets has been tethered to the use of cryptoassets. DeFi protocols generate fees from trading, lending, and derivatives activity that is itself denominated in cryptoassets, and those fees accrue back to tokens within the same closed ecosystem. The result is a system that expands and contracts with the market cycle. When sentiment is positive and prices are rising, activity flourishes and value accrues. When sentiment turns and prices fall, activity collapses and the cycle resets. This is cyclical growth.

The introduction of real-world assets has the potential to change that dynamic entirely. When tokenised Treasuries, equities, commodities, and private credit flow onto public blockchains, the activity those assets generate is no longer tied to the crypto cycle. Trading volumes, interest payments, and collateral flows from real-world assets are driven by economic fundamentals outside the crypto ecosystem. This is secular growth, and it is precisely what blockchain infrastructure has lacked until now.

The scale of the opportunity is difficult to overstate. Estimates place the total addressable market for assets that could eventually migrate on-chain at around USD850-trillion, spanning global equities, fixed income, commodities, real estate, and private markets. Capturing just 1% of that would put approximately sixteen times the value of the high-quality liquid assets currently on-chain to work within DeFi. Capturing 5% would put it at around forty times. These are not ambitious

projections. They are conservative thresholds relative to the size of the underlying markets. The direction of travel is clear enough. A small fraction of global financial assets migrating on-chain would represent a step-change for the industry.

For blockchain technology to evolve from an experimental financial layer into a sustainable economic system, it needs to support real, productive assets. Bringing real-world value, property, debt, equity, and intellectual capital onto public blockchains. These are the assets that drive employment, innovation, and economic output. If blockchain infrastructure is to fulfil its promise, it needs to mature to serve and enhance these real economic behaviours, not just financialise its own tokens.

Productive, on-chain assets shift blockchain's focus from internal speculation to external impact. They anchor DeFi to real-world demand, improve capital efficiency, and demonstrate the social utility of programmable finance. This is how blockchain earns its place in the next generation of global infrastructure. As a platform for meaningful, value-accretive economic activity rather than as a casino.

PART IV

Challenges

The promise of a new financial system is real and it is guarded by dragons. The technology has matured. The rails work. The early scaling problems are largely solved. What stands between today and a fully realised on-chain economy is a different set of obstacles. Some technical, some economic, some about the basic question of who has rights to what. Anyone investing in this space needs to understand these challenges clearly, because they are also the place where the next generation of value will be created or destroyed.

This chapter walks through five of them. The shift from counterparty risk to technical risk. The hyper-competitive structure of crypto markets. The unresolved question of token holder rights. The asset problem that is now DeFi's biggest constraint. And finally privacy and identity, which together gate the next wave of mainstream adoption.

The Shift from Counterparty Risk to Technical Risk

Legacy finance relies heavily on trusted intermediaries. Banks, brokers, custodians, and clearinghouses sit between every two parties to a transaction, facilitating the exchange and enforcing the agreement. This introduces counterparty risk to everything we do with our money. The danger that one party defaults on its

obligations, whether through insolvency, fraud, or mismanagement. Enforcement depends on social processes like legal contracts, regulatory oversight, and human-led dispute resolution. These can be slow, costly, and prone to bias or corruption.

Blockchain technology fundamentally reorients this dynamic. It replaces human intermediaries and social enforcement mechanisms with cryptography, economic incentives, and consensus protocols. DeFi protocols like Aave on the lending side, or Uniswap on the trading side, let users interact directly with self-executing code on blockchains like Ethereum. Trust is minimised because no single entity holds custody, and outcomes are determined deterministically through game-theoretic incentives like staking penalties for misbehaviour, and through network consensus where validators agree on transaction validity and guarantee finality.

These rails eliminate counterparty risk. They allow us to transact without needing to trust an intermediary or the social processes that hold that intermediary to account.

Blockchains do not eliminate risk altogether. They transform counterparty risk into technical risk, which is not the same as risk-free. Once deployed, smart contracts are immutable, which means bugs and vulnerabilities can lead to irreversible losses. There is no recourse when something goes wrong. You cannot call up Vitalik Buterin and ask him to roll back a botched payment. Audits, formal verification, and bug bounties help mitigate some of these issues but cannot eliminate them entirely. Code is written by humans, and unforeseen risks exist. This is an obvious barrier to adoption. Legacy finance relies on safeguards like recoverable human processes and recourse in the event that something does not go as planned.

Persistent exploits with declining relative impact

Technical risks remain a persistent threat in crypto, and the trajectory is clearly improving. According to Chainalysis and TRM Labs, in 2025 alone, total losses from hacks, exploits, and theft ranged from USD2.7-billion to USD3.4-billion. The majority of these losses were driven by centralised exchange breaches, including the USD1.5-billion Bybit hack, and by social engineering attacks rather than pure DeFi smart contract vulnerabilities.

Even as Total Value Locked has rebounded significantly, DeFi-specific losses have been notably suppressed compared to prior cycles. As of January 2026, global DeFi TVL stands at around USD100-billion to USD130-billion. Smart contract bugs accounted for a smaller share of losses in 2025, with most exploits occurring via off-chain vectors like private key compromises and phishing attacks. Smart contracts are evolving and maturing to risks. Earlier years saw exploits scale linearly with TVL growth. Improved tooling, better formal verification, timelocks, and multi-signature wallets have broken this relationship.

DEFI LOSSES RELATIVE TO TVL

Year	Total Crypto Losses (USD)	DeFi TVL Peak / Avg (USD)	DeFi Losses (USD)	Losses as % of Avg TVL
2022	3.8B	~200B / 120B	~3.0B	~2.5%
2023	1.7B	~100B / 60B	~1.0B	~1.7%
2024	~2.9-3.3B	~150B / 100B	~1.5B	~1.5%
2025	2.7-3.4B	~200B+ / 120-150B	~0.6-0.8B	~0.4-0.6%

Source: Chainalysis, DefiLlama, and Rekt.news

As a percentage of TVL, exploit losses have trended downward over time. Absolute figures remain elevated because the ecosystem is larger, and relative risk is materially lower than in DeFi's early days. One of the great features of blockchain's open-source nature is that many eyes tame complexity, and risks are constantly being identified and resolved.

For some investors, technical risk remains a deal breaker. Whether it is the bearer nature of cryptoassets or outsourcing the management of those assets to smart contracts, these risks are real and require vigilance. This gives us two paths forward. We either dismiss an emerging technology with enormous potential because there are risks, or we keep working toward making wallets, custody, and DeFi safer. I am an optimist. I believe we have the human intelligence and ingenuity to lower technical risk to parity with counterparty risk, and eventually reduce it to the point where interacting with a counterparty no longer makes sense.

Hyper Competition

Banks, payment networks, and custodians operate closed, permissioned systems protected by regulation, licensing requirements, and decades-old trusted relationships. A startup cannot simply plug into Fedwire. It needs approval, capital reserves, compliance infrastructure, and political connections that take years to secure, if it can secure them at all. Gatekeeping and high barriers to entry are a consequence of trust-maximised legacy finance.

For users, switching costs are punishing. Changing banks or brokers means time and money spent opening new accounts, setting up direct debits, running credit history checks, and completing KYC paperwork. Clients end up locked into

entrenched monopolies or oligopolies that extract rents far above what would be possible in a more competitive environment. These problems are amplified in the developing world.

Crypto turns this model upside down. Core DeFi protocols are open source, composable, and permissionless. Anyone can fork Uniswap or Aave in an afternoon and offer the same functionality with a few tweaks. Users face near-zero friction. A wallet connect, a couple of clicks, and they can be routed to the best price via a decentralised exchange aggregator. This is hyper competition. Far more intense than anything in traditional software, let alone finance.

For users, the outcome is unambiguously superior. Capital can flow to the most efficient venue in real time, fees compress quickly, and low barriers to entry sustain constant innovation. New capabilities appear regularly because no one needs permission to build on Ethereum. The dynamic mirrors the early internet's triumph over corporate intranets. Open protocols eat closed gardens because developers and liquidity naturally gravitate to where friction is lowest.

Investors face a challenging environment. Moats are shallow and temporary. Clever token incentive programmes can cause liquidity to migrate from venue to venue. Valuation remains difficult and feels speculative because sustainable technical competitive advantages are rare in a world where code can be copied and users are mercenary.

Even in the face of hyper competition, winner-take-most dynamics still emerge. Uniswap has been forked thousands of times, by Sushiswap, Pancakeswap, Quickswap, Aerodrome, and many others, and still commands around 40% of Ethereum DEX volumes. The same is true for Aave's core lending logic, which has been replicated and tinkered with endlessly, and continues to command more than 50% of active loans on Ethereum.

Network effects can take hold in DeFi, especially around liquidity and integrations. The best DeFi protocols quickly become infrastructure that developers build on top of rather than replace.

Token Holders vs Equity Holders

Tokens are new, unique assets we have never seen before. A single token can encapsulate multiple functionalities like service provision, governance, value distribution, and membership. This innovation is incompatible with existing securities laws. Ideally, ten years ago, regulators and industry participants would have sat down together and laid out the rules of the road. That is not how things played out.

The situation reached a climax during the Gensler era at the SEC from 2021 to 2025. Gensler led an openly hostile regulatory environment for US-based crypto projects, forcing a stark separation between equity holders, typically in entities like Uniswap Labs or Aave Labs, and token holders. The fear of tokens being classified as securities led teams to structure protocols in such a way that minimal value generated by the protocol would accrue to token holders, while equity captured upside from valuable IP, fee siphoning, and various side hustles. Bad incentives bred bad outcomes.

Venture funds and founders of DeFi protocols reaped the benefits of these poor incentives through salaries, advisory contracts, and various forms of off-chain revenue. Many DeFi tokens ended up as speculative bets without any claims on cash flows. Those claims do not need to be legal in nature. They can be

programmatic, either via a dividend or a buyback, or captured and allocated via governance of the protocol, often a decentralised autonomous organisation, or DAO.

Addressing this requires regulatory clarity for the crypto industry and its builders. The CLARITY Act will be a good first step in cleaning up token holder rights. Companies like Blockworks are also doing important work with their minimum disclosures framework and investor relations platform, which I think is integral for crypto to step into adulthood. There is no reason why DeFi protocols should not be able to follow similar value accrual methodologies as listed companies to maximise token holder value. They provide a service, charge a fee for that service, build up residual interest, and have governance structures to decide how that residual value is allocated. Incentives are key, and the separation between development labs and the DeFi protocol itself needs to be more clearly defined and aligned.

Investors have been silently protesting these distorted incentives. DeFi as a category was down 61% in 2025. These market signals, plus a less hostile regulatory environment, are paving the way for alignment. Examples of this can be found in recent proposals on the Uniswap and Aave governance forums.

Uniswap's UNIfication proposal, passed in late 2025, exemplifies progress on token holder rights by aligning Uniswap Labs with UNI holders. The proposal sought to activate protocol fees to burn UNI, retroactively burn 100-million UNI representing forgone fees since launch, funnel Unichain sequencer fees to burns, and shift the Lab's focus from interface monetisation to protocol growth. This is a massive victory for UNI holders and DeFi investors in general. UNI has transitioned from a governance token with no claims on the protocol's cash flows to a value-accruing token tied directly to the protocol's success.

Aave faces similar tensions that still need to be resolved. What excites me is that we are finally seeing these discussions on governance forums. The Aave token captures lending fees, and a 2025 proposal hinted at the issuance of new tokens that would inevitably dilute Aave token value and divert new business lines, like those focused on Real World Assets, into a newly issued token. Another incident, around Aave Labs absorbing trading fees from the user interface, caused some token holders to take to governance forums. The backlash to such proposals and actions is a signal that token holder rights are top of mind.

This is a boon for token investors. Market signals of plunging prices and community backlash are forcing improvements and will likely end the prolonged bear market in DeFi tokens.

Even with such progress, I remain concerned about the industry's current obsession with token buybacks. Buybacks are a straightforward way to align interests, and they are generally poor capital-allocation decisions for early-stage businesses. Most buyback programmes are fully programmatic, which means buybacks occur at any price on a periodic basis. This is not intelligent capital allocation. I am confident that the industry can move past buybacks as the primary alignment tool and move closer toward token holders actively participating in governance and placing their confidence in core developers' decisions regarding the protocol's future trajectory. This can only work if developer incentives are aligned with token holder interests.

The future of DeFi will come down to two things. First, achieving regulatory clarity so that operators have a clear line of sight into the industry's rules. Second, governance. Like corporations, token holders must support and hold to account DAO participants to steward capital wisely. Buybacks are quick fixes and a poor long-term strategy. They should be weighed up against R&D, bounty programmes, customer acquisition, and future development goals.

DeFi protocols do not need quick fixes. They need regulatory clarity and intelligent capital allocation. Achieving this alone would cause a rerating in DeFi token prices.

An Asset Problem, Not a Tech Problem

Blockchain technology has matured considerably since the peak of dot-crypto in late 2021. The technical problems, primarily the lack of scalability and smart contract risks, have largely been resolved. The problem now is a lack of quality assets. Without successfully capturing the new markets of stablecoins and real-world assets, these protocols could remain underutilised and continue to devolve into the zero-sum speculation that has plagued the industry since inception.

For DeFi to thrive, it must come to finance and manage productive assets. Those generating sustainable real yields, backing real value, and enabling long-term investor goals. DeFi needs to service assets that people actually care about and need.

DeFi's childhood has been impressive. Settlement volumes are in the trillions, TVL exceeds USD120-billion, and DEXs handle trillions of dollars in exchange volumes. Imagine onboarding the world's capital markets, like tokenised equities, bonds, or real estate. Servicing these markets would explode utilisation, turning protocols into global, always-available services like email, but for lending, borrowing, payments, and trading without borders.

Crypto's promise is trust-minimised finance. Replacing high rent-seeking intermediaries with open protocols to lower the global cost of capital, collapse low-trust economies' net interest margins, and eliminate layers of redundant work

estimated at USD9-trillion to USD29-trillion in trust-related social processes. Crypto is the new rail for a global property rights system that is more resilient, efficient, and inclusive.

Privacy and Identity

It turns out blockchains are too transparent. Every transaction is verifiable on an immutable ledger that anyone can read. This openness comes at a cost. It exposes sensitive details to the world, creating risks for individuals and barriers for businesses. If you pay for your coffee at Starbucks, the Starbucks employee could see your public key and use a block explorer like Etherscan to view your balances, spending habits, and associations. That could lead to terrible outcomes, including kidnapping and violence. Governments could use this transparency against their citizens as well, easily tracking donations, purchases, or affiliations, and eroding personal freedoms. For businesses, the problem is strategic. No business wants its trade secrets, supplier contracts, payroll, or strategic moves open to competitors.

Privacy on-chain is essential to the future of decentralised finance. The industry has been hard at work on solutions, and those solutions, once on the frontier of mathematics and cryptography, are beginning to mature.

The most important of these is the Zero-Knowledge Proof, or ZKP. A ZKP lets one party prove to another that a statement is true, for example "I own enough funds for this transfer", without revealing any of the underlying data like amounts or identities. Think of it as proving you are over 21 at a bar without showing your full ID. The bartender verifies the fact and learns nothing else. In blockchain, ZKPs use cryptography, often referred to as zk-SNARKs or zk-STARKs, to bundle transactions privately. The network confirms validity via succinct proofs, keeping

details hidden while maintaining ledger integrity. This preserves user privacy through anonymous transfers and firm confidentiality through confidential deals, while enabling scalability through batched verifications.

Privacy in crypto is not new. ZKPs were just frontier technologies, and Ethereum has always followed a safety-first approach. Zcash pioneered ZKPs for fully shielded transactions, hiding sender, receiver, and amounts since 2016. Ethereum Layer 2s like Aztec and Polygon zkEVM have already experimented with the tech for private DeFi, allowing for confidential lending and trading. Many other examples exist, and in 2026, ZKPs are coming to the Ethereum mainnet, where the bulk of action is happening. Vitalik Buterin, Ethereum's creator, is confident that ZKPs are ready for prime time.

Identity

Legacy finance requires users to surrender sensitive personal information to every financial intermediary they wish to deal with. This creates honey pots of private information for hackers and bad actors to exploit, and many such exploits have occurred. Once a user's personal information is shared, it is vulnerable forever, protected only by the individual entity's ability to protect it. This has led to countless instances of identity theft and fraud. For financial services providers, the burden is enormous. AML and crime compliance costs exceed USD200-billion annually, and fines for non-compliance, or for being slightly behind the curve in money laundering schemes, continue to grow.

The system also leaves many without access to financial services. The West enjoys a robust system of state-issued IDs enabling access, and the world is bigger than Western developed economies. According to the World Bank's 2021 Findex, 1.3-billion adults remain unbanked, in part because many developing economies lack formal identity systems, locking these individuals out of finance. Non-state-

issued identities could bridge this gap, giving the unbanked access to self-sovereign proofs to use financial services without relying on flawed government-issued credentials.

Blockchain and ZKPs could alleviate these issues. We can use blockchains to privately link verifiable credentials to public keys, removing KYC/AML barriers while enabling seamless access to financial services. Instead of re-issuing your private information endlessly, users could prove attributes once via ZKPs, like "I am over 18 and KYC-verified", without revealing the underlying details. Experiments already exist. Projects like Human Passport, with more than two-million users, offer ZK-based verification. This centralises nothing. Users control credentials in their own wallets, sharing proofs selectively across services.

On-chain identity would be another huge unlock for the broader DeFi ecosystem, making lending, trading, insurance, and remittances borderless and inclusive. We could develop credit scoring by analysing transaction history to quantify default risk without fully revealing all the data. Projects like Cred Protocol, Credora, and Gauntlet are already experimenting with this.

Each of these challenges is also where the next decade of value will be created. Lower technical risk attracts more conservative capital. Better token holder rights rerates the entire DeFi sector. More quality assets on-chain unlocks the protocols that already exist. Privacy and identity on-chain bring the rest of the world's users into the system. The dragons are real, and they are not impassable.

PART V

Investing in Crypto

Cryptoassets can be complex, and it is easy to get confused trying to understand them. Categorising cryptoassets is more nuanced than any simple breakdown, and a practical simplification helps clarify the key differences and how to approach them.

Most cryptoassets fall into two main categories. Crypto networks and crypto applications. These two types of cryptoassets are different enough in purpose, structure, and economics that investors find it useful to approach them differently.

Crypto networks are decentralised infrastructures. They coordinate a set of validators or miners to secure the system and provide foundational services like consensus, settlement, and transaction processing. Think of these networks as the financial equivalent of cloud infrastructure. A neutral foundation that applications rely on. Examples include Ethereum and Solana.

Crypto applications are decentralised services built on top of these networks. Rather than operating their own validator sets, they tap into an existing network's financial cloud to deliver specific services like exchanges, lending protocols, and asset management tools. Examples include Uniswap, which offers decentralised token swaps, Aave, a decentralised lending platform, and Raydium, a decentralised exchange and liquidity provider on Solana.

The defining feature that separates these two categories is whether the token is transactional or non-transactional. A transactional token is essential to the day-to-day operation of the network it services. The network cannot function without it. Ethereum's ETH and Solana's SOL are transactional. Every transaction, every loan, every swap consumes some of it as a fee to the validators securing the chain.

A non-transactional token is not required for the underlying protocol to operate. Uniswap's UNI, Aave's AAVE, and Raydium's RAY are all non-transactional. Uniswap would continue to facilitate swaps, and Aave would continue to facilitate loans, if their tokens ceased to exist tomorrow. This tells you something important. The value of a transactional token is anchored in the network's operational demand for it. The value of a non-transactional token has to be explicitly designed, through code-enforced mechanisms that pass protocol value back to tokenholders. Without that design, a non-transactional token is a claim on nothing.

Recognising this distinction helps investors better understand how each type of cryptoasset should be approached, where risks and rewards lie, and how best to assess their potential. The rest of this section walks through how to analyse each category in turn.

Crypto Networks

When we look at crypto networks like Bitcoin, Ethereum, or Solana from a traditional finance perspective, it is easy to fall into the trap of applying the same metrics we would use for companies like Apple, Amazon, or Meta. Crypto networks fundamentally differ from corporations in how they operate, generate value, and distribute it to participants. Recognising these differences is crucial for making sense of their investment potential and understanding why many conventional metrics do not map cleanly onto blockchain-based systems.

Networks are not companies

A traditional company has income, expenses, executives, employees, and clear lines of ownership. A decentralised crypto network has none of these in any recognisable form. It is closer to a protocol. Think of it like the internet itself. Nobody wonders whether the internet is profitable. It is simply an infrastructure that exists for anyone to use. The same goes for Bitcoin, Ethereum, or Solana. They provide essential services like consensus, settlement, and transaction processing, and they do not earn or lose money in the traditional sense.

Calling a crypto network profitable is misleading because there is no single, consolidated entity to which income or costs can be attributed. Instead, a broad community of miners, validators, developers, and tokenholders collectively sustains the network. The network's token may accrue value over time, and that is not the same as the network itself turning a profit, just as the internet does not claim profits when the value of internet-based companies rises.

What makes these networks genuinely novel is that their native tokens occupy a category of their own. A token like ETH possesses qualities of both a commodity and a capital asset, a combination that does not appear elsewhere in financial markets. As a commodity, ETH is consumed every time a transaction is processed, a loan is issued, or a swap is settled. Every time a user requires validity and finality for a transaction of value, ETH is burned as a fee. As a capital asset, ETH can be staked to earn a yield, similar in spirit to a bond coupon. Staking is not merely a return mechanism. It is the economic security layer of Ethereum itself. Validators must stake ETH as collateral to participate in consensus, and for that security mechanism to be meaningful, ETH must hold real value. A network secured by worthless collateral is no network at all.

This creates a reflexive relationship. The utility Ethereum provides depends on the security ETH underwrites, and that security depends on ETH retaining value. The same dynamic holds across proof-of-stake networks more broadly. It is a

structural feature of the asset class that traditional finance has no clean analogue for, and it is the reason valuation frameworks borrowed from equities or commodities alone tend to miss the point.

Tokenholder income and perspectives

Although crypto networks are not companies, many issue tokens that confer certain benefits or rights. The trick is identifying whose perspective you are measuring from.

In a proof-of-stake network like Ethereum, newly issued tokens are paid to stakers who help secure the chain. Those stakers effectively see issuance as income, whereas unstaked tokenholders experience that same issuance as dilution. Two holders of the same token can have completely different economic experiences of the same event, depending on whether they are actively contributing to network security.

Choosing the right reference point is essential. Some analysts consider the entire tokenholder base, staked and unstaked, as a single group and measure whether they gain or lose value through issuance in aggregate. From that viewpoint, if a network has high issuance and high demand driven by thriving network activity, the net impact on the total tokenholder base may still be positive. Others prefer to isolate the staker's economic position, which more closely resembles equity ownership with a yield attached.

It is worth pausing on that analogy. Proof-of-stake networks often behave more like equity than commodities. Stakers receive rewards similar to dividends and face potential dilution if they do not stake, which is reminiscent of the dynamic where shareholders who do not participate in a rights issue see their stake diluted. Proof-of-work networks like Bitcoin more closely resemble commodities. Newly issued

coins, like newly mined gold, do not automatically accrue to existing holders. They are distributed to miners based on computational work, and existing holders experience issuance purely as supply expansion.

Neither lens is wrong. They capture different facets of what a crypto network actually is.

The role of taxes

A frequent misconception is that token issuance itself constitutes a cost to the network because it creates sell pressure from stakers paying taxes on their newly minted tokens. While it is true that tax events can prompt some holders to sell a portion of their rewards to cover liabilities, this does not reduce the fundamental value of the network or its token. It is comparable to equity holders paying personal taxes on stock dividends, which does not affect the intrinsic value of the corporation issuing those dividends.

In the current regulatory climate, many jurisdictions treat newly issued tokens as taxable income despite the fact that this often resembles a stock split more than a genuine profit distribution. That tax treatment is inconvenient and arguably illogical, and it does influence short-term investor behaviour. It does not diminish the network's value in a global context. Because crypto is borderless, participants can choose more favourable jurisdictions or use alternative token formats like non-rebasing liquid staking tokens to minimise tax friction.

Analysing a crypto network's health or investment potential means recalibrating our mental models. Instead of looking for corporate-style profit-and-loss statements, we need to examine the factors that actually drive network value. Token demand, the capital the network secures, adoption, real-world demand for its blockspace, and the monetary activity flowing through it. The protocols themselves do not make money, and they may generate substantial value for the ecosystem of tokenholders, developers, and users who rely on their infrastructure. Understanding

these nuances is key to approaching crypto networks with a sharper, more informed investment lens. The chapter on Useful Metrics and Relative Value Analysis returns to these factors in more detail.

Crypto Applications

Whereas crypto networks defy traditional notions of profit and loss, crypto applications more closely resemble conventional businesses in how they generate revenue. Built on top of crypto networks, these applications deliver services like exchanges, lending platforms, asset management strategies, and derivatives markets, and typically charge a fee in return. In this sense, they are easier to assess using familiar finance constructs. You can examine revenues, costs, capital allocation decisions, and growth metrics to gauge their performance.

A useful mental model here is the vending machine. A vending machine aggregates a supply of chips, cold drinks, and chocolate bars from various suppliers. People walk past, and every now and then, someone stops and buys a snack. The machine's total sales are its fees, accumulated in its money box. The machine's first line of costs is paying the suppliers, the providers of the chips and chocolate bars. Whatever is left is the machine's revenue, and what is paid out to the machine's owners is the owner's revenue.

With a few different words, this is exactly how crypto applications work. They aggregate capital on the supply side, which they use to service demand. A decentralised exchange aggregates paired-token liquidity from liquidity providers and services traders who want to swap tokens. A lending protocol aggregates loanable capital from depositors and services borrowers. A derivatives platform aggregates risk capital from liquidity providers and services traders seeking leveraged exposure. A liquid staking protocol aggregates validator infrastructure

from operators and services tokenholders who want staking rewards without running their own nodes. What varies between applications is the shelf contents, not the underlying mechanics.

Each interaction charges a fee, and those fees flow through a predictable waterfall.

Gross merchandise value generates fees. Fees split between the supply side and the protocol itself. What the protocol retains is its revenue. And what the protocol then chooses to pass through to tokenholders, if anything, is holder revenue.

This is where crypto applications start to look less like conventional businesses. A traditional company that generates revenue has a clear structure of ownership, and shareholders have legal claims on that revenue through dividends or retained earnings that accrue to book value. Crypto applications have no such structure. The application itself is a set of smart contracts, not a company. The token associated with it is not equity, and tokenholders do not hold legal claims on the protocol's assets or revenues. This distinction matters enormously. The fact that a protocol generates hundreds of millions of dollars in fees tells you nothing, on its own, about whether any of that value reaches you as a tokenholder.

The only claims that can exist on a crypto application are those that are code-enforced. A smart contract that routes a portion of protocol revenue to tokenholders as a stablecoin dividend, a buyback that uses protocol earnings to purchase tokens on the open market, or a burn that permanently removes tokens from circulation. These are the mechanisms that translate protocol success into tokenholder value. Without them, a protocol can be wildly profitable while its token is, in economic terms, a claim on nothing.

This is the single most important lens through which to evaluate a crypto application. Does protocol success actually reach you? The answer lies in the token's design, specifically in the code that governs how value flows from gross

fees down to the tokenholder. The chapter on Useful Metrics and Relative Value Analysis returns to this in detail, introducing ratios like the protocol take rate and holder take rate that allow investors to measure these flows directly.

Governance, alignment, and novel ownership models

Despite the absence of traditional legal claims, crypto applications have developed their own governance structures, typically in the form of decentralised autonomous organisations (DAOs). A DAO issues its own token, and tokenholders have the right to propose and vote on changes. In effect, this functions as a global, continuous shareholders' meeting. Tokenholders can influence everything from fee rates and product roadmaps to capital allocation decisions, including whether the protocol reinvests its revenues into development, distributes them to tokenholders, or accumulates them in a treasury.

What sets crypto applications apart from conventional businesses is the possibility of direct user ownership and alignment. Platforms can reward the supply side, like liquidity providers or validators, with governance tokens, turning them from mere users into partial owners. They can offer discounts to tokenholders, airdrop tokens to superusers, and host worldwide governance votes to shape protocol direction. These tactics cultivate an ecosystem where loyalty is rewarded and the boundary between customers and investors blurs.

Token-based governance also allows for fluid and global participation. In a traditional enterprise, only accredited or local investors might be able to buy shares, and shareholders typically meet once a year for a formal Annual General Meeting. A crypto application can grant near-instant governance rights to anyone who holds its token, no matter where they live, sparking rapid iteration and stronger network effects.

Crypto applications are still rooted in familiar economic realities. Revenue, user adoption, and operational efficiency matter here as much as they do anywhere else. What makes them distinct is the combination of open infrastructure, programmable value flows, and decentralised ownership models that allow them to build more global, transparent, and user-aligned services than their traditional counterparts. For an investor, the critical question is always the same. The protocol may be a cash machine, and the question is whether any of that cash is reaching you.

Useful Metrics and Relative Value Analysis

There is no Intelligent Investor or Fixed Income Handbook for cryptoassets. The industry itself has not yet agreed on a universal valuation methodology, and it often struggles to define even the most basic financial metrics consistently. Part of the difficulty lies in the sheer novelty of the asset class. Cryptoassets do not map cleanly onto equities, bonds, commodities, or currencies. They possess features of several of these categories simultaneously, and forcing them into any single bucket loses something essential about what they actually are.

This is the single biggest pitfall an investor can bring to crypto analysis. The temptation to reach for a familiar lens, equity multiples, bond yields, commodity supply-and-demand, is strong precisely because these frameworks are rigorous, widely understood, and comforting. Applying a framework designed for one asset class to something genuinely new produces confident-sounding conclusions built on the wrong foundations. The investor who values ETH purely as a share of a growth-stage tech company will reach a very different conclusion to the one who values it purely as a digital commodity, and both will miss most of what makes ETH interesting in the first place.

The right starting point is to recognise the novelty honestly. Crypto networks and crypto applications are two different kinds of things, and they each demand their own analytical approach. Crypto applications have enough in common with traditional businesses that conventional tools like revenue analysis, margin examination, capital allocation decisions, and discounted cash flow modelling can be adapted with care. Crypto networks, by contrast, resist conventional categorisation almost entirely. They behave less like companies and more like economies, and they need to be assessed as such. The rest of this section walks through both challenges in turn, starting with the harder one.

A closing note before we get into it. Valuation in crypto remains genuinely contested. There is no consensus on which lens is the dominant lens. Different market participants value these assets through different frameworks, and prices at any given moment reflect the weighted influence of those competing views. The most rigorous approach is not to pick a single framework and defend it to the last. It is to understand how the major lenses work, recognise which ones apply to which assets, and hold a balanced view of where consensus may form. This is the mindset the rest of this section is written to support.

Analysing crypto networks

Before discussing specific metrics, it helps to internalise what a crypto network actually is. It is not a company. It is not a platform in the conventional sense. It is closer, in both structure and behaviour, to an emerging economy. Participants transact, contracts are executed, capital is deployed and withdrawn, and activity rises and falls with the cycles of economic expansion and contraction. Like any economy, its health cannot be captured by a single number. It is assessed through a dashboard of indicators that together describe the level and direction of activity.

This framing changes what investors should look for. Rather than searching for a single valuation multiple, the goal is to build a multi-angle view of the network's economic throughput. Because crypto networks operate on public, open ledgers, almost everything is directly measurable in real time.

The starting point is raw usage. Daily active users, transaction counts, aggregate settlement volumes, total value locked in smart contracts, and the amount of stablecoins and tokenised real-world assets circulating on the network are all direct indicators of adoption. Each of these speaks to a different dimension of network activity. User counts capture the breadth of participation. Transaction counts capture the intensity of use. Settlement volumes capture the value being moved. Total value locked captures the capital that has chosen the network as its home for productive deployment. Stablecoin and tokenised asset market caps capture how much real-world monetary and economic value is using the network as settlement infrastructure.

That last point deserves emphasis. As tokenisation accelerates, the addressable value that crypto networks can service expands. More stablecoins issued on a network, more tokenised Treasuries, equities, and commodities flowing across it, means more opportunities for the network to service real economic demand. A network hosting USD5-billion in tokenised assets serves a fundamentally smaller economy than a network hosting USD500-billion. The direction of travel matters here, and the tokenised assets data from the chapter on Real World Assets translates directly into a forward-looking metric for network health.

Beyond raw usage statistics, a network's fees and settlement flows form something like its gross domestic product. When an exchange, lending protocol, or derivatives platform charges a fee, that fee reflects a real economic exchange of value. Aggregated across the network and all the applications running on it, this gives you a concrete measure of the economic activity the network hosts. Growing ecosystem fees and settlement volume usually indicate a growing blockchain economy.

Measuring this properly requires distinguishing between what the network itself captures and what flows through its broader ecosystem. Jon Charbonneau at DBA has done useful work on the first part of that picture, focusing on the fees and MEV (miner or validator extractable value) that accrue directly to the network. Two of his measures are Total Economic Value (TEV), defined as the sum of network fees, MEV tips, and token issuance, and Real Economic Value (REV), which excludes issuance and focuses on just network fees plus MEV tips. Both let investors compare networks on a like-for-like basis, which is especially useful in proof-of-stake ecosystems where inflationary token rewards can otherwise distort the picture.

These measures are valuable, and they capture only what the network itself extracts. A more complete view of a blockchain economy also has to include the activity flowing through it. A useful framing here is Total Economic Activity, which adds two further inputs to the network-level picture. It combines chain fees and MEV, settlement volume moving across the network, and the fees generated by applications built on top. This gives a fuller sense of a blockchain's scale as an economic platform, capturing both what it directly extracts and what it enables for others. It sits naturally alongside TEV and REV and, on balance, is closer to the GDP framing of a network's total output.

A further layer of analysis comes from multiple-based metrics that draw on a historical cost basis. MVRV (Market Value to Realised Value), introduced by David Puell and Murad Mahmudov, contrasts a cryptoasset's total market capitalisation with its realised cap, which values each token at the price at which it last moved on-chain. MVRV fluctuations give investors a sense of whether the market is overextended or undervalued relative to historical patterns of holder profitability. Net Unrealised Profit/Loss (NUPL) captures the difference between realised and unrealised profits across the entire token supply, offering insight into how many of the network's holders are in profit and whether a market cycle might be nearing a top or a bottom.

All of these tools acknowledge the essential reality of crypto networks. They operate as open global platforms where usage, adoption, and economic throughput can be measured directly via on-chain records. No single metric perfectly captures a network's intrinsic value, and together they provide a framework for understanding activity levels, comparing networks against each other, and gauging cyclical shifts in sentiment.

There is one more layer worth discussing. The native tokens of crypto networks are not pure commodities and not pure capital assets. They sit somewhere in between. They possess features of both, and that duality is central to valuing them. Take ETH as the clearest example. As a commodity, ETH is consumed every time a transaction is processed, a loan is issued, or a trade is settled on Ethereum. It behaves like digital oil. A consumable resource that powers economic activity. Its supply dynamics reinforce this framing. ETH's issuance rate is algorithmically determined and offset by its consumption through network usage, giving it a high stock-to-flow ratio that places it squarely in the range of gold and far above that of industrial commodities. At the same time, ETH is also a capital asset. It can be staked to earn yield, in a way that looks and feels like an income stream. That yield is not incidental. It is the mechanism by which Ethereum's economic security is maintained, and it is the reason the asset behaves partly like an equity or a bond.

This is the dual lens through which network tokens should be assessed. They are not commodities alone, not capital assets alone, but a genuinely new category that requires both frames simultaneously. Investors who pick only one of these lenses, because it feels familiar, will miss at least half of what drives the asset's value.

Analysing a crypto network means treating it as a living economy whose health and value emerge from the ever-evolving interplay of users, applications, capital, and on-chain economic dynamics. The goal is not to land on a single number. It is to develop a grounded view of where the economy is in its cycle, what direction it is moving in, and whether the assets that power it are appropriately valued relative to the activity they support.

Analysing crypto applications

Crypto applications sit on the more familiar side of the analytical divide. They generate revenue, incur costs, make capital allocation decisions, and can be assessed through tools adapted from traditional equity analysis. That familiarity is also a trap. The fact that a protocol is profitable tells you nothing, on its own, about whether any of that profit reaches you as a tokenholder. The work of analysing a crypto application is two-sided. You need to assess the underlying business, and you need to assess whether the token itself is a credible claim on that business.

The right starting point is the token rights framework. Before reaching for any metric, an investor should run four questions through every token they consider.

THE TOKEN RIGHTS FRAMEWORK

Four questions to run every token through

01 **What rewards exist?**

What does the token actually entitle you to? The possibilities typically fall into one of four categories. Inflationary rewards paid in the token itself, a share of protocol revenue, governance rights, or some combination of the three. Many tokens confer none of these in any meaningful sense, which is itself an important finding.

02 **How do you access those rewards?**

Rewards are rarely automatic. Most require staking or locking tokens. Hard lockups commit tokens for a fixed period and carry liquidity risk. Soft lockups allow free exit, sometimes after a short cooldown, and do not.

03 **How do the rewards reach you?**

Dividends in stablecoins deliver stable value and create taxable events. Buybacks avoid the taxable event and are vulnerable to front-running. Burns are cleanest in tax terms and forgo treasury diversification. Treasury accumulation gives the DAO flexibility at the cost of holder returns.

04 **How is any of this enforced?**

Tokenholders have no legal claims on protocol assets or revenues. The only claims that exist are those that are code-enforced and programmatically executed. If the mechanism depends on a DAO vote that could reverse it, the claim is softer than it appears.

Running every token through these four questions before analysing any metric will tell you whether you are looking at a genuine claim on something or a claim on nothing.

METRICS THAT MATTER

Once you have established what the token actually is, the metrics start to make sense. The most important ones are all variations on the theme of measuring how much protocol value actually reaches tokenholders.

- **Protocol take rate (protocol revenue ÷ fees).** This ratio measures what percentage of top-line fees the protocol itself captures, as opposed to passing through to the supply side. A decentralised exchange might generate significant trading volume and fees, and if the majority of those fees flow to liquidity providers rather than the protocol itself, the protocol's effective top line is much smaller than its headline fee number suggests. Protocol take rates vary widely. Early-stage protocols often keep them low to bootstrap growth, essentially subsidising the supply side with retained value. Mature protocols with strong market positions can push take rates significantly higher because their network effects protect them from supply-side competition.
- **Holder take rate (holder revenue ÷ protocol revenue).** This is where things get interesting. The holder take rate measures what portion of protocol revenue actually reaches tokenholders through code-enforced mechanisms. It is here that the difference between a well-designed token and a poorly designed token becomes visible in the numbers. A protocol can retain significant revenue from its fees while returning none of it to tokenholders, making the token a claim on nothing despite the protocol's apparent health. Some protocols pass through effectively all of their protocol revenue to tokenholders, making the token an almost pure claim on the business.
- **Outstanding FDV to holder revenue (P/HR).** This is the closest thing crypto has to a price-to-earnings ratio. It compares the fully diluted value of the token to the annualised revenue that actually reaches holders. It is the single

most useful multiple for comparing crypto applications, and it is far more honest than the more commonly cited price-to-fees or price-to-protocol-revenue multiples. The reason is straightforward. Price-to-fees tells you how the token is priced relative to the top line of a business that may or may not be passing anything through to you. Price-to-holder-revenue tells you how the token is priced relative to the cash flows you actually have a code-enforced claim on. The difference can be dramatic. A token that looks cheap on a price-to-fees basis can be meaningfully more expensive on a price-to-holder-revenue basis, sometimes by multiples. Investors who rely only on headline fee multiples will systematically underestimate how expensive poorly-designed tokens actually are.

- **Future dilution (outstanding supply ÷ maximum supply).** Not all tokens in existence are in circulation. Early-stage protocols typically reserve significant portions of their total supply for future emissions, team vesting, investor unlocks, and community rewards. A token where only a small fraction of the total supply is in circulation carries meaningful future dilution risk, and that risk should be priced in. This is not necessarily a disqualifier. Early-stage protocols that are using emissions to bootstrap growth may be allocating capital intelligently. Ongoing unlocks can trigger market events as new supply reaches circulation, and investors need to be confident that the dilution is being put to productive use.

Together, these four metrics allow an investor to triangulate the real economic position of a crypto application token. A protocol with a strong take rate, a high holder take rate, a reasonable P/HR multiple, and a largely circulating supply is very different from one with a strong take rate, a zero holder take rate, and significant future dilution ahead. The first is a claim on a growing business. The second is a speculation on governance and narrative.

GROWTH EXPECTATIONS AS A DISCIPLINE

Forecasting the future cash flows of a crypto application five years out is genuinely difficult. The sector moves quickly, competitive dynamics shift, governance decisions can reshape economics overnight, and regulatory developments can expand or compress the market in either direction. A traditional discounted cash flow model, which requires confident assumptions about future revenue, margins, and terminal value, often collapses under the weight of that uncertainty.

A more useful exercise is to run the logic in reverse. Rather than forecasting growth and solving for price, take the current price as given and solve for the growth rate the market is implying. This is sometimes called reverse DCF, or expectations investing. It replaces the question "what is this token worth?" with the more tractable question "what does the market need to believe about this protocol for the current price to make sense?"

The approach is mechanical. Take the current fully diluted valuation. Take the current annualised holder revenue. Apply a discount rate and a terminal growth assumption, and solve for the revenue growth rate that would make the DCF equal to the current market price. The result is the implied growth rate, expressed as a compound annual rate over your chosen projection period.

Running this exercise at three different discount rates is more informative than running it at one. A low discount rate, perhaps 8 to 10%, reflects the kind of return an investor might demand for a mature, cash-flowing business with clear competitive moats. A moderate rate of around 15 to 20% reflects the risk profile of a growth-stage technology business in a well-established sector. An aggressive rate, perhaps 25 to 30% or higher, reflects the reality that crypto applications are early-stage, competitively exposed, and subject to both execution risk and regulatory risk that traditional equities do not face.

The spread between these three implied growth rates tells you something important. A token might look reasonable at an 8% discount rate and require growth rates that border on implausible once you apply a discount rate appropriate to the actual risk profile. Crypto investors should be discounting aggressively. The risks are real, the sector is young, and the opportunity cost of capital within the asset class is high. A token that requires 40% annual growth in holder revenue for a decade, discounted at 25%, to justify its current price, is not cheap. It is priced for a specific, demanding future, and the investor's job is to assess whether that future is realistic.

This reframing changes the analytical goal. Instead of producing a target price, the investor produces a distribution of implied expectations across a range of risk assumptions. That distribution can then be tested against everything else in the analysis. Is the implied growth rate consistent with the protocol's historical trajectory? Is it consistent with the overall size of the market the protocol serves? Is it consistent with what competing protocols are doing? The current price is not a conclusion. It is a hypothesis the market has made about the future, and the investor's job is to decide whether to accept or reject it.

PART VI

State of Cryptoasset Regulation

United States

The regulatory landscape for crypto assets in the US has transformed significantly since early 2025. The posture has moved from regulation-by-enforcement to active legislative engagement. The shift began in January 2025 when President Trump signed an executive order to promote US leadership in digital financial technology, prohibit central bank digital currencies (CBDCs), and establish the President's Working Group on Digital Asset Markets. Two months later, a further executive order created a Strategic Bitcoin Reserve and Digital Asset Stockpile, making the US the first major economy to hold Bitcoin as a strategic government asset.

The most consequential development came in July 2025 with the signing of the Guiding and Establishing National Innovation for US Stablecoins Act, known as the GENIUS Act. This was the first piece of federal digital asset legislation ever enacted in the US. It establishes a comprehensive regulatory framework for payment stablecoins, requiring full one-to-one backing by US Dollars or other low-risk assets, imposing reserve transparency and redemption requirements on issuers, and carving compliant stablecoins out of the federal definitions of security and

commodity. The effect was immediate. Major banks including JPMorgan, Citi, and Bank of New York Mellon accelerated their on-chain efforts, and the stablecoin market expanded materially in the months following passage.

Alongside GENIUS, Congress has been working to resolve the broader question of market structure. The Digital Asset Market Clarity Act, known as the CLARITY Act, passed the House of Representatives in July 2025 with a bipartisan 294 to 134 vote. It would grant the Commodity Futures Trading Commission (CFTC) exclusive jurisdiction over digital commodity spot markets, resolving much of the jurisdictional ambiguity that has defined the US approach for years. As of early 2026, the bill is still making its way through the Senate, where the Banking and Agriculture Committees have each published their own versions. Industry observers expect a narrow path to passage before the midterm election cycle consumes the legislative calendar.

The SEC has also reoriented. Under new leadership, the commission has stepped back from its enforcement-heavy posture, dropping several high-profile cases inherited from the previous administration and establishing a Crypto Task Force focused on proactive rulemaking. State-level fragmentation remains, with New York's BitLicense regime still among the most stringent in the country, and the federal direction of travel is now clear. The United States is moving from ambiguity toward a structured framework designed to balance innovation with consumer protection, positioning itself as one of the leading jurisdictions in the global crypto economy.

United Kingdom

The UK is in the final stages of building a comprehensive regulatory framework for cryptoassets, and the timeline has extended beyond initial expectations. HM Treasury is classifying cryptoassets as specified investments under the Financial

Services and Markets Act 2000 (FSMA), which expands the Financial Conduct Authority's (FCA) oversight to issuance, custody, lending, staking, and related activities. The framework applies to both domestic and offshore firms servicing UK clients, narrowing exceptions for reverse solicitation and raising standards around transparency and consumer protection.

The legislative foundation was laid in December 2025, when the government placed the draft Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2025 before Parliament. The FCA is now finalising the accompanying rulebook through a series of consultation papers covering trading platforms, intermediation, prudential requirements, and stablecoin regulation. Final rules are expected in summer 2026, with concluding perimeter guidance to follow in autumn. The authorisation gateway for firms will open on 30 September 2026, and the full regime is scheduled to commence on 25 October 2027.

This timeline creates meaningful compliance pressure. Firms that wish to continue offering regulated cryptoasset services to UK clients must apply during the gateway window, or risk losing the benefit of transitional provisions when the regime takes effect. Many market participants had expected a later start date for applications, and the earlier-than-anticipated opening has prompted industry groups to flag that firms need to begin preparing substantially earlier than originally planned.

On specific activities, the government has abandoned plans to regulate stablecoins under a separate payments framework in favour of a unified approach within the broader crypto regime. Staking services have been clarified out of the classification as collective investment schemes through legislative amendments finalised in January 2025, providing welcome clarity for validators and liquid staking protocols.

Separately, the Cryptoasset Reporting Framework (CARF) came into effect in January 2026, imposing due diligence and reporting obligations on service providers to combat tax evasion. Users must self-certify their tax residency, and non-compliance carries meaningful penalties. Taken together, these measures represent one of the more comprehensive attempts by a major jurisdiction to integrate cryptoassets into an established financial regulatory architecture. The UK is positioning itself as a credible, rules-based venue for the sector.

United Arab Emirates

The UAE has built one of the most advanced regulatory frameworks for cryptoassets globally. It combines federal oversight with emirate-specific authorities to create a multi-layered but coherent structure. At the federal level, the Central Bank of the UAE (CBUAE) oversees stablecoins and payment tokens under its Payment Token Services Regulation, which took effect in July 2024. The regulation prohibits carrying out payment token services without a licence and restricts payments in virtual assets to either UAE Dirham-denominated stablecoins or non-Dirham tokens issued by a CBUAE-licensed issuer. The Securities and Commodities Authority (SCA) regulates tokenised securities and investment tokens under federal law, coordinating closely with emirate-level regulators.

Dubai's Virtual Assets Regulatory Authority (VARA) remains the most active and influential cryptoasset regulator in the region. In May 2025, VARA published Version 2.0 of its complete Rulebook framework, which took effect in June after a short transition period. The updates tightened controls around margin trading, introduced a sponsored VASP regime, and overhauled the issuance framework by creating distinct categories. Category 1 covers Fiat-Referenced Virtual Assets (FRVAs) like stablecoins and Asset-Referenced Virtual Assets (ARVAs) backed by real-world assets like real estate or commodities. Category 1 issuances now require

prior VARA approval and carry full reserve and disclosure obligations. Category 2 covers most other tokens, including governance and utility tokens, which do not need a direct licence and must be placed or distributed through licensed distributors. By February 2026, VARA had fully implemented FATF Travel Rule requirements, mandating originator and beneficiary information for all VASP transfers.

The financial free zones continue to complement this framework with specialised regimes. The ADGM's Financial Services Regulatory Authority (FSRA) operates one of the longest-established digital asset rulebooks globally and introduced new product intervention powers in January 2026 to restrict specific crypto derivatives that pose systemic risk. The DIFC's Dubai Financial Services Authority (DFSA) has recognised multiple tokens and stablecoins, including Ripple's RLUSD, and in January 2026 moved to a firm-led suitability assessment model that places greater responsibility on licensed firms to justify token suitability. RAK Digital Assets Oasis continues to offer a dedicated free zone with tax incentives for cryptoasset firms.

The direction of travel is clear. The UAE is positioning itself as a fully regulated institutional hub rather than a sandbox. Its removal from the FATF grey list in February 2024 and the EU's AML high-risk list in July 2025 has strengthened its credibility with global institutional capital. For firms weighing where to base crypto-related activity, the combination of clear rules, active regulators, and a well-developed free zone ecosystem makes the UAE one of the most compelling jurisdictions available.

European Union

The EU's regulatory framework for cryptoassets reached a major milestone with the full implementation of the Markets in Crypto-Assets Regulation (MiCA) on 30 December 2024. MiCA establishes a harmonised regime across all 27 EU member states, replacing fragmented national rules and introducing a unified licensing system for crypto-asset service providers (CASPs). The framework covers a broad range of cryptoassets, including exchange tokens like Bitcoin, utility tokens, and stablecoins, while excluding non-fungible tokens unless they function similarly to other cryptoassets. Key requirements include strict reserve obligations for stablecoin issuers, consumer protection measures, and environmental impact disclosures.

By early 2026, the enforcement phase is well underway. More than 40 CASPs have been authorised across member states, with the Netherlands, Germany, and Malta leading in issuances. Major global exchanges have secured licences through EU entities, often after overhauling their European operations to meet MiCA's governance, custody, and reserve requirements. Stablecoins that do not meet MiCA's standards have been delisted from compliant platforms. The transitional period during which existing providers can continue operating under national regimes varies by member state, and the EU-wide backstop is 1 July 2026. After that date, any entity providing crypto-asset services to EU clients without a MiCA licence will be in breach of EU law.

Supervision is layered. The European Securities and Markets Authority (ESMA) leads on supervisory convergence, market integrity, and the public register of authorised CASPs. The European Banking Authority (EBA) focuses on stablecoins, including prudential and reserve requirements for Asset-Referenced Tokens (ARTs) and E-Money Tokens (EMTs), with direct supervisory powers over tokens deemed systemically significant. National competent authorities grant CASP authorisations and enforce breaches within their jurisdictions.

Complementary regulations reinforce MiCA's objectives. The Transfer of Funds Regulation requires traceability of crypto transactions, mandating sender and beneficiary details to combat money laundering. The Digital Operational Resilience Act (DORA) strengthens IT risk management for financial entities, including crypto firms, and has been in full application since January 2025.

The market impact has been significant. EU-regulated exchange volume initially declined as non-compliant products were withdrawn, and established institutions like Société Générale entered the stablecoin market directly with fully regulated EMTs. Challenges remain, particularly around decentralised finance and the treatment of activities that do not fit neatly into the CASP taxonomy. MiCA has achieved what it set out to do. It has created legal certainty, passporting rights, and a credible framework for institutional participation. As the most comprehensive crypto regulation implemented by any major economic bloc, it is also influencing regulatory design in other jurisdictions, from the UK to Singapore to the UAE.

South Africa

South Africa's cryptoasset regulatory framework has evolved significantly since 2022, integrating cryptoassets into existing financial legislation rather than creating standalone laws. Cryptoassets are classified as financial products under the Financial Advisory and Intermediary Services Act (FAIS Act), requiring Crypto Asset Service Providers (CASPs) to obtain Financial Services Provider licences from the Financial Sector Conduct Authority (FSCA). The licensing regime has been actively enforced. As of early 2026, the FSCA had received 512 applications, of which 300 were approved, 14 declined, and 121 withdrawn following engagement with the regulator. The authority has made clear that any entity conducting CASP-related activities without a licence will face enforcement action.

Amendments to the Financial Intelligence Centre Act (FICA) designate CASPs as accountable institutions, enforcing anti-money laundering protocols, customer due diligence, and suspicious transaction reporting. Directive 9, effective 30 April 2025, implemented the FATF Travel Rule, requiring CASPs to collect and transmit originator and beneficiary details for transactions exceeding R5,000. CASPs must also establish Risk Management and Compliance Programmes under Section 42 of FICA. NFTs and stablecoins remain outside the current regulatory definition, leaving them unregulated despite growing market activity.

The most significant recent development is international in nature. On 24 October 2025, the FATF removed South Africa from its grey list after the country completed all 22 action items required by its action plan. The European Union followed by removing South Africa from its High-Risk Third Country Jurisdictions list with effect from 29 January 2026. The crypto regulatory infrastructure built during the grey-listing period, particularly the FICA amendments and Directive 9, was central to securing the delisting, and it has now become a durable part of the country's financial architecture. South Africa's next full FATF mutual evaluation is scheduled to commence in the first half of 2026 and conclude in October 2027, which means compliance standards are unlikely to relax.

The National Treasury has published the draft Capital Flow Management Regulations 2026 for public comment, with submissions due by 10 June 2026. These regulations propose to bring cryptoassets expressly within South Africa's exchange control framework for the first time, replacing the Exchange Control Regulations of 1961. A new category of authorised crypto asset service provider (ACASP) is proposed, similar to the existing authorised dealer regime for foreign currency, requiring Treasury authorisation for CASPs facilitating cross-border capital flows using cryptoassets. This closes one of the most significant gaps in the current framework, the ability of crypto to effectively circumvent exchange controls on offshore capital movement.

The South African Reserve Bank's exploration of a wholesale central bank digital currency remains tentative, with progress slow. The overall regulatory direction is clear. South Africa is moving from a reactive, gap-filling regime toward a comprehensive framework that brings crypto into alignment with the country's broader financial and exchange control architecture.

> *“Bitcoin is math, and math has been around for thousands of years. I like the idea of investing in something that is reliable, consistent, honest, and 100% certain.”*
>
> — PAUL TUDOR JONES

ABOUT THE AUTHOR

Jason Carpenter is the founder of Etherbridge, a liquid long-only cryptoasset fund. He publishes research under the Chain Street brand and writes on Bitcoin, Ethereum, decentralised finance, and the emerging agentic economy. He holds an MSc in Blockchain and Digital Currency from the University of Nicosia and is a CFA Level I candidate.

etherbridge.co · chainstreet.substack.com