CLEARTOKEN

White Paper

The Case for a Central Securities Depository for Digital Assets

Chapter Two:

The Future of Finality

September 2025

The Future of Finality in Digital Assets

Every trade must conclude in the same way: both parties receive what they are owed, and legal ownership is transferred to the buyer.

Every market depends on the same principle: once something has changed hands, it stays that way. Transactions must be final.

In essence, **settlement finality is the assurance that once a transaction is settled, it is legally and operationally irreversible, even in the event of insolvency.** Without this certainty, a single default can ripple outward; undermining trust, freezing markets, and escalating into systemic risk.

In traditional finance, **financial market infrastructures** (FMIs) - central securities depositories (CSDs), payment systems and clearing houses (CCPs) - are **legislatively empowered** to operate the systems which alone can establish finality and establish ownership.[2-1]

On the other hand, the financial philosophy of decentralised finance (DeFi) holds a central belief: "***code is law***". Its core technology, blockchain, uses cryptographic methods to make transaction reversal computationally prohibitive, and as such, DeFi advocates claim finality through blockchain's two headline benefits: an **immutable** and **irrevocable ledger.**

Trust on such typically community-led, peer-to-peer public blockchains is not a matter of reputation, balance sheets or legal fallback, but is based in the platform's performance. However, while blockchain can provide strong operational assurances, **neither ownership nor finality are concepts of code, but of law.**

Therefore, the compatibility of blockchain technology with existing legal and regulatory requirements, and its impact on participants and systemic resilience, requires deep scrutiny.

For digital assets to thrive, the two must work in tandem: private blockchain ensures technical integrity, while legal frameworks establish enforceable finality.

As we continue to examine the case for a CSD for digital assets, this chapter will explore how **digital assets can benefit from unconditionally enforceable and irrevocable settlement finality** against the backdrop of these critical concerns and evolving regulatory landscape.

Chapter Summary

1. **Blockchain cannot deliver legal finality without legal recognition.**
   Despite claims of immutability, blockchain transactions remain vulnerable to reversal, dispute, or legal challenge without enforceable legal frameworks.

2. **The absence of legal finality exposes digital asset markets to systemic risk.**
   Without recognised settlement systems, insolvency, fraud, or operational failure can unwind trades, freeze assets, and trigger contagion across markets.

3. **Institutions cannot operate in markets without enforceable ownership and title.**
   Legal clarity around asset ownership, jurisdiction, and enforceability is essential for institutional adoption, collateral use, and cross-border scalability.

4. **A CSD for digital assets is essential to deliver trust, finality, and systemic resilience.**
   Only a legally recognised CSD can provide the infrastructure needed to guarantee settlement finality, protect against clawbacks, and support institutional growth.

The Foundation of Trust:
Immutable & Irrevocable; The Ledger Must Not Be Changed

Evolving from hefty books to electronic records, well-governed ledgers have recorded securities ownership since shares were first issued in 17th century Amsterdam. Accepted as the single source of truth, irrevocable ledgers remain a cornerstone of market confidence.

An *irrevocable* ledger ensures that once a transaction is recorded it cannot be undone or reversed. This provides a permanent, secure and transparent record of ownership. In traditional finance (TradFi), securities ledgers are typically managed by central securities depositories (CSDs), whose legal recognition establishes its position as the single source of truth.

DeFi advocates seek to eliminate such intermediaries through using distributed ledger technology (DLT), to argue that code can enforce irrevocable ledgers by making them ***immutable*, meaning that the transaction records cannot be altered.**

Blockchain Immutability is Technical, Not Legal

Blockchain, the most prominent DLT, confirms transactions in a 'block' using cryptographic protections.

As further blocks are added to the chain, altering the record retrospectively becomes computationally prohibitive. For example, after six subsequent blocks have been confirmed on the Bitcoin network, transactions are widely considered 'settled' and 'final'. This is **not because reversal is impossible**, but because it would require extraordinary computational effort, making reversal highly improbable.

Additionally, the ledger is distributed across the network of nodes that each maintain a copy. Changes require their consensus, further guarding against record tampering. This leads proponents to regard blockchain as a '*golden source of truth*', despite its lack of legal recognition. However, while blockchain is often described as immutable, **this immutability is technically probabilistic, not legally absolute. This distinction is critical.**

Finality is a Legal Concept

In regulated markets, settlement finality must be irrevocable and unconditional, not just enforceable, or reversable, through lengthy court cases. Legal certainty cannot be left to post-trade interpretation, especially given the severe implications of multiple claims to assets, particularly when used as collateral.

Global financial market infrastructures adhere to the Bank for International Settlement's *Principles for FMIs* (PFMIs), of which the first standard is establishing their legal basis (*see below*). Public blockchains are not FMIs and do not adhere to these principles, nor benefit from their protections.

Principles for Financial Market Infrastructures (PFMIs)

Principle 1: Legal Basis [3-1]

"An FMI should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions."

Key considerations

1. *The legal basis should provide a high degree of certainty for each material aspect of an FMI's activities in all relevant jurisdictions.*
2. *An FMI should have rules, procedures, and contracts that are clear, understandable, and consistent with relevant laws and regulations.*
3. *An FMI should be able to articulate the legal basis for its activities to relevant authorities, participants, and, where relevant, participants' customers, in a clear and understandable way.*
4. *An FMI should have rules, procedures, and contracts that are enforceable in all relevant jurisdictions. There should be a high degree of certainty that actions taken by the FMI under such rules and procedures will not be voided, reversed, or subject to stays.*
5. *An FMI conducting business in multiple jurisdictions should identify and mitigate the risks arising from any potential conflict of laws across jurisdictions.*

Explanatory note

3.1.1 *A robust legal basis for an FMI's activities in all relevant jurisdictions is critical to an FMI's overall soundness. The legal basis defines, or provides the foundation for relevant parties to define, the rights and obligations of the FMI, its participants, and other relevant parties, such as its participants' customers, custodians, settlement banks, and service providers. Most risk-management mechanisms are based on assumptions about the manner and time at which these rights and obligations arise through the FMI. Therefore, if risk management is to be sound and effective, the enforceability of rights and obligations relating to an FMI and its risk management should be established with a high degree of certainty.* ***If the legal basis for an FMI's activities and operations is inadequate, uncertain, or opaque, then the FMI, its participants, and their customers may face unintended, uncertain, or unmanageable credit or liquidity risks, which may also create or amplify systemic risks.***

If It Can Be Forked, Can It Be Trusted To be Final?

Unfortunately, the assurance of 'block confirmation' is not absolute and even technically "settled" transactions can be rewritten. For example, when a blockchain undergoes a significant reorganisation or 'hard fork', previously confirmed blocks and their associated transactions can be replaced with an alternative chain, **potentially duplicating and/or unwinding transactions once believed to be immutable; complete, final and irreversible**.

Blockchain Alone Cannot Guarantee Finality: The Chain Can be Changed

Forks can arise for several reasons:

- Protocol upgrades that require changes incompatible with the existing chain.
- Disagreements among developers or validators over governance, direction, or consensus rules.
- Security breaches or exploits, where rollback is proposed to recover stolen funds.
- Ideological splits, where communities diverge over principles like immutability or decentralisation.

Whilst hard forks necessitated by technical updates can be scheduled into the future, they can also be used to rewrite the past.

Significant Ethereum and Bitcoin Forks

The **2016 DAO hack on Ethereum** is a well-known example of such a hard fork with major market impact (*see the first white paper in this series, "Bridging the TradFi-DeFi Gap: The Future of Finance Depends on Traditional Trust and Regulation", for an in-depth look).*

In short, to recover $60 million in ETH stolen from the DAO group of 11,000 investors, the majority of the Ethereum community voted with the founders and key developers' lead to roll back the blockchain to before the hack and invalidate previously confirmed transactions to before the theft occurred.

This caused a split in the community as many believed this contradicted the core DeFi principles of blockchain immutability. Ethereum was **hard forked** into two distinct chains: Ethereum (with the rollback) and Ethereum Classic (preserving the original record).

Bitcoin has also had significant hard forks. Bitcoin Cash split off in 2017, which itself soon forked in 2018 into two competing chains: Bitcoin Cash and Bitcoin Cash SV (Satoshi's Vision).

Each fork arose from development communities being unable to agree a singular philosophical or technical approach to block sizes, transaction costs and scalability in line with the original Bitcoin white paper.

The Problem of Unaccountable Authority

While forks are often framed as community-led governance decisions, they expose a deeper vulnerability: **the ability to rewrite history**.

Critically, the authority behind these decisions is often undefined, unaccountable, and opaque. There is no regulator, no court, and no formal process, just a loose consensus among developers, miners, or token holders. This means that, even without malicious intent, asset ownership can be reversed by actors who may not be known, elected, or subject to oversight, exposing participants and their assets to risks beyond their control.

In regulated markets, such uncertainty is unacceptable. Finality must be enforceable, not subject to ideological votes or technical reorganisation. **Without legal recognition, blockchain immutability remains a technical feature, not a legal guarantee.**

Blockchain splits aren't limited to major events like hard forks that are managed by the protocol's governance: benign errors and network latency can cause temporary competing chains. More serious, are deliberate attacks.

The Threat of 51% Attacks

This malicious strategy exploits the decentralised nature of blockchain consensus, which typically requires a majority (at least 51%) of mining or validation power to confirm transactions.

Put simply, an **attacker gains control of this majority to force an alternative chain of fraudulent records**. Holding the majority of validation power enables them to operate at high speed to beat out legitimate miners' blocks and cause the network to adopt their longer chain. This triggers the block reorganisation mechanism, designed to determine legitimacy where blocks have been mined more than once.

This allows the attacker to create and delete previously confirmed transactions and rewrite transaction history. As a result, they can use the same funds in two different transactions, known as **double-spending**.

Similar to the impact on Participant A in the illustrative example below, double-spending causes significant losses for exchanges and users who accepted transactions that were later invalidated. For example:

- **Ethereum Classic** (2020): two successful 51% attacks resulted in losses of over $7 million of ETC in just a week:
  - **1st August:** 3,693 blocks were reorganised, resulting in 807,000 ETC (~$5.6m) being double-spent, along with 13,000 ETC in mining rewards.[5-1]
  - **6th August:** 4,236 blocks were reorganized, leading to around 465,000 ETC (~$1.68m) being double-spent.[5-2]

  These were swiftly followed by a third attack on 29th August, in which over 7,000 blocks were reorganised, losing an unconfirmed amount.[5-3]
- **Bitcoin SV** (2021): The attack erased 570,000 transactions from around 100 blocks on the smallest of the three bitcoin chains,[5-4] resulting in three versions of the blockchain being mined simultaneously.[5-5]

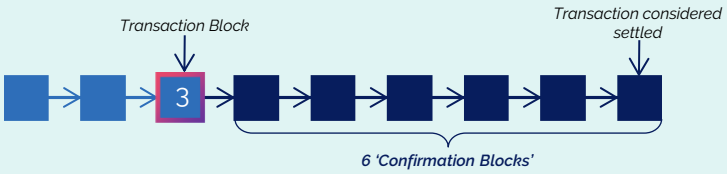
As the attack unfolds, nodes may become uncertain about which blocks to reject as fraudulent, leading to further chain splits and network instability. During this period, the ledger cannot be trusted, and participants are unable to trade safely due to the risk of transaction reversal and inconsistent state.

51% Control: The Ability to Rewrite History

Participant A buys BTC for USD from Participant B

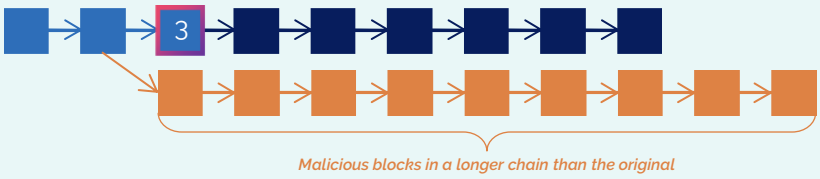
The transaction transferring BTC ownership from B to A is reported in Block 3.

6 confirmation blocks follow: the trade is considered settled and final.



A 51% attack was also underway…

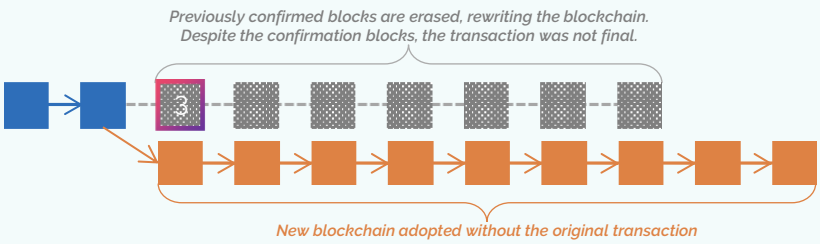
Nodes follow the longest valid chain, so the attacker creates a longer chain than the original from an earlier block (Block 3). By gaining sufficient hashing or validation power, the attacker can cause the network to reorganise around their version, making it the canonical chain and potentially reversing previous transactions.



The new record

The blockchain reorganisation invalidates the valid chain's blocks, including Block 3.

This enables the attacker to double-spend (reusing the same funds in both chains) by invalidating previously confirmed transactions and replacing them with conflicting ones.



The new blockchain history no longer reflects Participant A's ownership of BTC; it reverted to Participant B, but B already received the cash payment through the digital exchange.

The potential consequences for Participants A and B are significant:

- Participant A may have moved or sold the BTC prior to the attack. The new record erases their ownership, meaning that A sold BTC that is no longer recorded as being in their possession.
- Reversing the cash (or other cryptocurrency) leg of the transaction may prove impossible, particularly if Participant B has already withdrawn or used the cash sent by Participant A.
- If the BTC purchase cannot be restored to the blockchain, Participant A faces a potentially unrecoverable cash loss.

The fork may take the participants to court to resolve the issue.

As this example demonstrates, code cannot be regarded as law.

Blockchain Forks and the Problem of Duplicate Records

Blockchain forks can create conflicting versions of the ledger, each containing a valid copy of the same asset. Without a central authority to determine and enforce legitimacy, both records may be considered equally valid. This poses serious challenges for legal certainty and enforceable ownership.

In decentralised systems, legitimacy is often established through continued community support. Developers, exchanges, and users collectively signal which version they recognise as authoritative. In some cases, an issuer of a digital asset inherent to the chain itself (e.g. a stablecoin provider) can unilaterally declare which chain is valid, making duplicates a minor inconvenience.

Real-World Assets Cannot Be Double-Spent

This approach breaks down when digital assets represent claims to real-world assets, such as shares, bonds or property. Unlike native blockchain assets like bitcoin, which can fork into two distinct tokens, **off-chain claims cannot be duplicated**. Two records representing the same legal entitlement are not just confusing, they are legally unacceptable.

Legal Certainty Requires Defined Governance

The *Principles for Financial Market Infrastructures* (PFMIs) establish that legal certainty must be grounded in a clear legal basis (PFMI 1, *see page 3*). Without a central coordinator or rulebook to determine and enforce legitimacy, the integrity of legal finality is absent, and forks can undermine blockchain settlement.

Financial Markets Depend on Immediate Finality

Courts may be forced to decide which record prevails, a process that could take several years. This **is highly incompatible with the immediate certainty required for financial markets**. Delayed resolution may, at best, keep assets locked. At worst, being unable to access assets, especially when used as collateral, creates systemic issues leading to mass insolvencies.

Blockchain Alone Is Not Enough

This highlights the insufficiency of blockchain alone for settlement. Legally recognised FMI, such as a digital CSD, is essential to resolve conflicts, ensure enforceable ownership and uphold finality. Without it, the risks of duplication, delay and dispute remain unresolved.

Breaking Trust Has Consequences

51% attacks are a known vulnerability of proof-of-work (PoW) blockchains. While the power required to execute the attack makes it economically unviable on most proof-of-stake (PoS) platforms, they remain a credible threat to smaller PoS networks.

However, any type of fraud and manipulation of the blockchain (whether through consensus attacks, protocol exploits, or governance failures), has serious implications for the digital asset ecosystem. Trust in coins, platforms and exchanges can be rapidly eroded, with lasting consequences for adoption and market stability. For example:

- Miners withdrew their support for Ethereum Classic after each 51% attack, making it increasingly easier for hackers to 51% attack the network.
- After the third Ethereum Classic attack, Coinbase increased ETC **"**deposit and withdrawal confirmation time**"** (i.e. settlement time) to 336 hours, which is around 2 weeks.[6-1]
- Several exchanges subsequently delisted and dropped wallet support for Bitcoin SV.

The absence of truly simultaneous and final settlement introduces risks that extend far beyond individual disputes or financial losses. **It undermines the perception of trust**, in turn discouraging both institutional and retail participation.

These attacks challenge the ability of blockchains to prevent double-spending without relying on a trusted intermediary. While some networks have moved to proof-of-stake consensus to mitigate these risks, that presents its own concerns, particularly around the concentration of power among large validators.

These are workarounds, not solutions. When a blockchain fails to deliver the immutability and irrevocability expected of it, the only recourse is often to reverse the ledger or suffer the loss.

Although legal action is likely to be taken in the event of significant hacks, with fewer avenues for recourse and unclear legal protections, a blockchain alone, arguably, cannot offer true finality as recognised in TradFi.

Legal remedies take time. In the interim, the issue becomes operational: markets freeze, trades are suspended and confidence collapse. This delay in resolution is what makes such systems unviable for institutional use.

Finality must mean final.

Governance Requires Permissioned Infrastructure

In institutional markets, governance must be clear, accountable, and enforceable. Public, permissionless blockchains often rely on pseudonymous actors, informal consensus, and opaque decision-making, leaving participants exposed to unpredictable changes and unresolvable disputes.

By contrast, private, permissioned blockchains offer a controlled environment where access is restricted to trusted participants, and governance rules are transparent, auditable, and legally recognisable. The possibilities of forking and 51% attacks are also eliminated.

Several institutions have now established 'semi-public' chains. By controlling all or a portion of Layer 1, the institution maintains control over protocol changes, transaction reversals, and dispute resolution, not anonymous consensus.

Notable examples include Canton Network (Global Synchronizer Foundation – a consortium of market leaders), Arc (Circle), Tempo (Stripe), BASE (Coinbase) and VTAP (Visa Tokenized Asset Platform).

They reinforce how institutions are increasingly designing blockchain infrastructure with governance embedded from the outset, ensuring compliance, stability, and legal clarity; key requirements for regulated financial markets.

Settlement Finality is a Legal, Not Technological, Concept

It Is Legislation That Enforces Transaction Irrevocability, Not Code

Probabilistic finality does not equate to legal finality: legislation enforces settlement finality, *not* ledger immutability. Whatever the underpinning technology or theoretical ethos, without legal protection, asset ownership and trade irreversibility rely on hope, not trust.

Why? Because they can be unwound in court.

What Does It Mean To Settle A Trade?

Trade settlement involves the successful exchange of cash and assets between buyer and seller according to the terms agreed when executing the trade. If one, or both sides, of the trade fail to deliver on their obligations, settlement is considered failed until the exchange has been completed.

Importantly, the legal or beneficial title of the asset should be transferred from the seller to the buyer in order to complete settlement.

Not All **Settled** Trades Are Automatically ***Final*** Trades...

- > *Book entry alone does not guarantee the transfer of legal or beneficial title to the buyer.*
- > *Ledgers only offer finality when legally recognised and empowered to do so.*
- > *Trades that are not legally final can be ordered to be unwound by a court judgement*

Understanding Settlement Finality

Establishing The Legal Principle of Finality

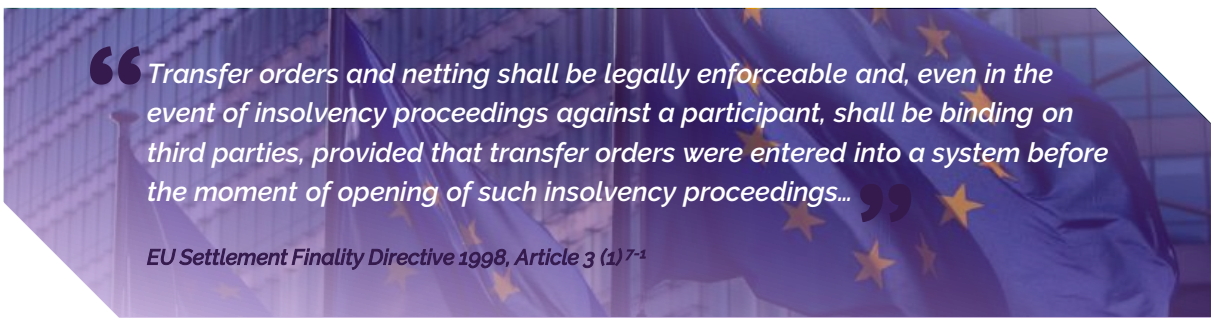
The international gold standard for settlement finality is articulated in the EU's Settlement Finality Directive (SFD), which has been adopted or mirrored in legislation across many jurisdictions, including the UK (and retained post-Brexit). Under the SFD, **a transfer order becomes legally protected once it has entered the designated settlement system**, shielding it from reversal even in insolvency proceedings.

Settlement finality ensures that **once a transaction is completed in a designated settlement system, it is legally irrevocable**, safeguarding participants from retroactive claims. This concept, foundational to traditional securities markets, is crucial for trust and stability.

The SFD stipulated that a **designated settlement system must execute the final transfers of cash and assets** through the book entry system and commercial or central bank ledger. This guarantees that:

- *Settlements cannot be unpicked or undone.*
- *Parties' rights are protected from the moment of settlement initiation through to completion.*
- *Title transfer orders cannot be revoked nor amended.*
- *Transferred assets (including collateral, repos) cannot be claimed by others, even in insolvency cases.*
- *Trade settlements are truly final, unconditional and irrevocable.*[7-1]

This protection is not theoretical. Without finality, every transaction carries the latent risk of reversal, especially in the face of insolvency.



> *"Transfer orders and netting shall be legally enforceable and, even in the event of insolvency proceedings against a participant, shall be binding on third parties, provided that transfer orders were entered into a system before the moment of opening of such insolvency proceedings..."*
>
> ***EU Settlement Finality Directive 1998, Article 3 (1)*** [7-1]

A Foundation of Finality: Indisputable Title – Legal & Beneficial

Title is a critical, though often assumed, pillar underpinning the operation of financial markets. It establishes rightful ownership of assets, the legal authority to transfer and dispose of them, and the responsibility for compliance with legal and regulatory obligations.

Legal title, (and in jurisdictions under English common law, beneficial title), provides certainty and enforceability, enabling smooth market operations and mitigating systemic risk. **Without it, disputes arise, market integrity erodes, and trust collapses.**

What is Legal Property?

There are currently two types of property under English common law:

Tangible	&	**Intangible**
"Things in possession" that have a physical presence: e.g. houses, cars		"Things in action" that contractually denote rights: e.g. debt claim

This clarity embedded in the legal framework ensures that rights over an asset are unambiguous, irrevocable and enforceable in court. **Such certainty is essential for any functioning market.**

How Ownership of Property is Legally Asserted & Enforced

Enforceable ownership of legally classified property is managed through title. Whether for cars, houses, or securities, legal title must be updated to reflect the transfer of ownership. This process is final and legally binding, and courts rely on evidence of title to clarify ownership and provide a basis for enforcement.

In the UK, government-mandated registrars manage these updates: just as the Land Registry manages property ownership, **securities transfers are overseen by legally recognised FMI called central securities depositories** (CSDs).

In traditional finance, CSDs play a critical role as neutral intermediaries, maintaining accurate records and transferring title during settlements. CSDs are empowered to settle with finality and serve as the 'single source of truth' for securities ownership, instilling confidence in markets.

The Impact of Legal and Beneficial Title

There is a **distinction between legal and beneficial titles.** The legal title holder is named as the formal owner, while the beneficial title holder enjoys the economic benefits, even if they do not directly control the asset. This important distinction in title allows collateral to be held and immobilised by a CSD or custodian, whilst remaining the property of the beneficial owner.

By virtue of trust law, the beneficial title holder retains the right to benefit from the securities, such as receiving dividends, interest, or other financial benefits and can make instructions enforceable through the intermediary holding the legal title.

This also establishes strong legal protection for the legal owner should their assets be stolen or otherwise misappropriated.

Possession of the asset does not equate to ownership.

How Is Title Managed for Digital Assets?

The regulatory framework applied to an asset (traditional or digital) depends on its classification under current legal definitions. This determines how it must be processed for settlement, and with it, how title is transferred.

For example, if a cryptoasset qualifies under existing definitions of transferrable securities, it falls under the MiFID II regime in Europe, enacted by FSMA 2000 and the Regulated Activities Order in the UK.

English common law has recognised *cryptoassets* (*see right*) as property, and court cases have affirmed their capacity to be being owned, transferred, and used as collateral. However, they are not accepted as either a physical or an enforceable contractual claim, outside of the current two definitions of property.

To add complexity, there is great diversity in digital asset types and the variation of their classifications across jurisdictions.

Digital Asset or Cryptoasset?

While often used interchangeably, cryptoassets and digital assets are not the same.

Cryptoassets typically refer to decentralised, permissionless tokens like bitcoin and Ethereum, often governed by public blockchains and where ownership is conferred through private cryptographic keys rather than book-entry systems.

Digital assets, in contrast, include tokenised securities, stablecoins, and other instruments that may be issued, traded, and settled within regulated environments and are generally not held as bearer instruments.

In this paper, 'digital assets' refers to both cryptoassets and tokenised financial instruments.

While cryptoassets like bitcoin and Ethereum are part of this category, our focus is on the infrastructure needed to support institutional-grade digital asset markets.

Possession vs Ownership: The Challenge for Digital Assets

In DeFi, which takes the "code is law" approach, ownership is tied to the control of a digital wallet via its private key. In the original Bitcoin whitepaper, Satoshi Nakamoto states:

> *"Each owner transfers the coin to the next by digitally signing... the public key of the next owner... A payee can verify the signatures to verify the chain of ownership."*[9-1]

This describes possession-based control, encapsulated in the popular phrase: "*Not your key, not your crypto*".

Whether or not the possessor is considered to be the 'rightful' owner, the blockchain will accept transactions from whoever has the valid key without checking why they have the key or whether they should have it; the blockchain only checks that they *do* have it. Therefore, loss, theft or compromise of the key often results in permanent loss of access.

This approach is problematic. **Key possession is not universally recognised as conferring legal title**, and stolen keys raise disputes over whether title remains with the original owner or transfers to the new possessor.

Another popular adage, "*possession is nine-tenths of the law*", highlights the limits of possession as legal entitlement to an asset. **Whilst possession can prove evidence of ownership, better title claim will win out.** Without a clear means of establishing enforceable title in digital assets, the onus is on the victim to prove that the assets were originally theirs and that they have the stronger claim to the asset.

Disputes over stolen keys or fraudulent transfers highlight the inadequacy of relying solely on technical controls and why DeFi's reliance on private keys is inadequate for institutions.

Currently, no government-mandated registrar or CSD exists for digital assets. Without a legally recognised ledger to register asset ownership, courts have often equated control of a private key to ownership, just like **bearer instruments**.

In Reality, Law is Law

The lack of such a definitive adjudicator or enforceable ownership means that error, fraud, or theft cannot be reliably resolved. Tulip Trading's case (*see right*) highlights the tension between legal ownership of digital assets and the technical reality that control is determined by access to private keys. **Even a DeFi evangelist who claims to be the creator of bitcoin turned to the court when something went wrong**, a clear contradiction to the "code is law" ethos.

The digital asset market cannot have it both ways. To function at institutional scale, infrastructure must align with the standards of legal and financial systems. Without a central authority or legal infrastructure to enforce rights, ownership effectively becomes unenforceable when keys are lost or stolen.

Digital assets need to be recognised as property and organised under a legal system that can clearly distinguish and enforce both legal and beneficial ownership and provide a consistent framework. Without this clarity, disputes (including cross-border) are difficult to resolve, assets cannot be reliably used as collateral, and market liquidity suffers, especially in institutional settings where title certainty is essential.

Fortunately, legal clarity is coming to the UK through the combination of two key developments: the Financial Services and Markets Act 2023, which defined a "cryptoasset" as "*any cryptographically secured digital representation of value or contractual rights...*";[9-2] and the forthcoming Property (Digital Assets etc) Bill, which will formally recognise digital property when it likely becomes law in late 2025.

Test Case: Tulip Trading vs Bitcoin Developers

In February 2020, Dr Craig Wright (who controversially claims to be Bitcoin creator Satoshi Nakamoto) lost access to 111,000 bitcoin owned by his company, Tulip Trading, through a hack that allegedly either stole or erased his private keys.[9-3]

Tulip Trading **sued a group of Bitcoin developers**, arguing that they had both the ability and obligation to alter the blockchain to restore access to the lost bitcoin.

The claim rested on the assertion that developers are the only parties capable of remedying such harm and therefore owe fiduciary-like duties to users of the network, particularly in cases of theft or loss. Without such duties, Tulip argued, the notion of legal ownership of digital assets is hollow if no one can enforce your rights when you're hacked.

Arguments central to the defence included:

- **Decentralisation:** Bitcoin's decentralised nature precludes any single party from controlling the network. Developers cannot compel miners or users to adopt changes, and the system operates by consensus, not command.
- **Lack of legal entity:** Bitcoin is not a legal entity, but an open-source collective of undefined volunteers. Assigning legal responsibility akin to that of formal trustees is therefore unrealistic.
- **Open-source licensing:** Bitcoin software is released under the MIT license which explicitly disclaims warranties and liability, reinforcing the argument that developers cannot be held responsible for user losses.

Although the case was initially dismissed, the UK Court of Appeal ruled in 2023 that the question of whether the "*fluctuating, and unidentified body*" of developers owe a legal duty was sufficiently novel and significant to warrant a full trial.[9-4]

Tulip Trading ultimately withdrew the case in April 2024, but **the door remains open for future legal challenges**.

The case encapsulates a fundamental tension between traditional legal concepts of property and the code-based autonomy of decentralised finance.

In conventional systems, enforceability of ownership rights relies on formal governance structures or legal intermediaries, such as banks or regulated FMIs, that can intervene when assets are lost or stolen.

In contrast, decentralised networks lack these mechanisms. Without legal title, custodianship, or enforceable remedies, the notion of ownership potentially changes: if no one can restore access or uphold rights after a hack, **what does it truly mean to "own" a digital asset?**

A Third Kind of Property

The UK is leading the way in establishing a legal foundation for digital assets within the common law system through the Property (Digital Assets Etc.) Bill (*see below*). This approach affirms the recognition of a **new, third category of personal property**, distinct from traditional classifications, which is particularly suited to the unique characteristics of digital assets.

By deliberately leaving the boundaries of this category to be developed by the courts, the UK ensures a flexible and adaptive legal framework that can evolve alongside technological innovation.

UK Property (Digital Assets etc.) Bill

Commonly referred to as the Digital Property Bill, this is a landmark initiative aiming to update property law to accommodate digital assets.

The Bill introduces a third category of personal property to cover digital assets which are neither physical tangible nor contractually intangible.

It gives digital assets clear legal status and protections, affirms their capacity to be owned, transferred, recognised and have rights enforced over them, including their use as loan collateral.[10-1]

At the time of writing, the Bill is progressing through Parliament.[10-2]

Financial Services and Markets Act (Regulated Activities etc.) 2000 – (Amendment) Order 2025

Proposed in April 2025, the Amendment is a draft statutory instrument laid before Parliament. It aims to bring certain digital asset activities within the scope of regulated financial services.[10-3]

Once enacted, it will enable the Financial Conduct Authority (FCA) to make rules, give guidance, and register entities for temporary permissions.

The Order will come into full regulatory effect 12 months after its initial commencement date.

Mine or My Custodian's?

As far back as the Dutch East India Company, share certificates were immobilised in a vault while ownership transfers were recorded through book-entry movements in ledgers. This foundation endures today: custodians and brokers hold **legal title to securities on behalf of beneficial owners, whilst CSDs enact the final transfer of ownership.**

This allows custodians to immobilise assets and efficiently transfer and settle transactions securely, whilst preventing double pledging or unauthorised use of assets. Simultaneous investor retention of beneficial title instils confidence that their rights are preserved, even without physical possession of their assets.

This custodial model offers both legal certainty and operational convenience, demonstrating the necessity of clear legal frameworks to define each party's rights, including entitlement to economic rights, recourse in disputes, and protections in insolvency.

The Implications for Digital Assets

By contrast, the current legal ambiguity in digital assets has serious consequences for institutional adoption and participant safety. For example:

- Unclear ownership: In many jurisdictions, it remains unclear whether depositing tokens with an exchange constitutes a transfer of ownership or merely a contractual claim. Several digital asset platforms (including cryptocurrency exchanges) claimed legal title to customer assets during insolvency proceedings, despite having marketed those assets as "yours" and "safely held" (*see Celsius case study on page 13*).
- Key instruments made unviable: Repurchase agreements (repos) are widely used for short-term liquidity and rely on the title transfer of collateral to the lender.
- Questionable enforceability: Unclear or contestable ownership poses serious risks to market stability. Such ambiguity can contribute to systemic contagion in highly interconnected markets.

For digital assets to support institutional adoption, market integrity, and cross-border enforceability, establishing and managing legal title recognition is imperative to build trust, embed resiliency and support growth.

The Need for a CSD

Modern financial markets orchestrate billions of asset transfers daily. **The importance of clear legal ownership and mechanisms for registering and transferring legal title cannot be overstated.**

In traditional market infrastructure, **CSDs fulfil that role, allowing participants to operate within a framework of certainty**. This is supported by its function in ensuring delivery versus payment (DvP) settlement: the simultaneous delivery of securities and cash. Once recorded, the trade is considered final and irreversible, even in bankruptcy, under the system's legal framework.

This legal certainty underpins trust and supports the scale and resilience of modern capital markets. In fact, the CSD may hold beneficial interests on behalf of custodians, who hold further beneficial interest on behalf of clients and so on.

It is very clear that despite any recognition as property, legal finality will remain elusive without a CSD for digital assets. Without enforceable legal structures and the market structure to support them, assurances of ownership are hollow.

Containing Contagion:
Why Finality is Fundamental For Every Trade, and Every Market

Systemic risk arises, not because of one participant failing, but the spread of that failure through obligations which cannot be met and the resulting loss of counterparty confidence. Stability in complex interconnected markets depends on the ability to contain failure.

Legally-recognised settlement finality ensures that once a trade has settled within a designated system, neither cash payments nor securities transactions can be reversed by subsequent claims or legal proceedings. Delivered through FMI, like CSDs, CCPs and payment systems, these protections guarantee enforceability by the end of the settlement date.

The rules governing finality, netting, and collateral enforceability are not theoretical constructs, they are active safeguards. They protect final transactions against retroactive claims, disputes, reversal, collateral invalidation, and the unwinding of settled obligations (i.e. 'clawbacks') in the event of insolvency.

Finality: The Anchor of Market Resilience

In complex interconnected markets, finality is the legal anchor that holds the system together under stress, actively guarding against market disruption and preventing systemic contagion.

Digital assets currently lack this anchor.

Blockchain platforms may offer technical assurances, but without legal enforcement or FMI designation, they lack the foundation required to instil trust and support scalable institutional participation. Institutions need to operate with confidence, knowing that their positions are secure and cannot be undone.

The Implications of Insolvency

Whether physically exchanging paper certificates or sending cryptoassets to a digital wallet: without a designated CSD, or equivalent recognised settlement system, a trade may be considered 'complete', but not legally final. Without enforceable finality, transactions have no **protection from insolvency clawbacks and can be challenged in court**. This introduces two material risks:

- Transactions can be unwound, and
- The system may grind to a halt as legal claims cascade through interconnected obligations.

To prevent this contagion, markets depend on the explicitly enforceable security of knowing that once a trade is settled, it cannot be undone for any reason.

Netting: Containment through Consolidation

In today's interconnected markets, risk containment depends on more than just the irrevocability of individual trades. The essential process of **netting compresses thousands of bilateral transactions into a single multilateral obligation**, consolidating settlement complexity and improving market efficiency.

If netting were to be undone to isolate the transactions of a defaulting participant, it would force the unwinding of vast volumes of previously settled trades. Such an event could have disproportionate repercussions and destabilise the entire market. Therefore, the finality of netted trades is explicitly protected in legislation; ensuring that the failure of one participant does not unravel the entire system.

Why Legal Infrastructure Matters

Digital asset markets currently have no CSD to operate a legally recognised settlement system, therefore, there is no mechanism to settle with legal finality and guarantee that trades cannot be unwound.

CSDs are explicitly tasked with enforcing the point of entry and irrevocability of trades, making them essential infrastructure for systemic risk mitigation.

This is why intervention is needed; not to restrict innovation, but to establish the legal infrastructure that enables it. Without recognised systems guaranteeing enforceable finality, markets remain exposed to systemic risk, and institutions cannot participate safely.

Core Legal Requirements for Settlement Systems Currently Absent in Digital Assets

Moment of Irrevocability

Settlement systems define the precise moment a transfer order is entered into the system at which point it cannot be reversed. *(Article 39, CSDR)*

Legal Enforceability

Transfer orders and their netting must be legally enforceable, including in insolvency proceedings. *(Article 3(1)–(2), SFD)*

Protection Against Retroactivity

Insolvency proceedings must not have retroactive effects on settled transactions entered before insolvency began. *(Article 3(1), SFD)*

Collateral Security Validity

Collateral used in settlement must be legally enforceable and protected from retroactive invalidation. *(Article 9, SFD)*

Recognised System Rules

The system's internal rules must be legally binding and define transfer and netting processes clearly. *(Article 2(a), SFD; Article 18, CSDR)*

Participant Protection

Participants in the system are protected from third-party claims that may challenge a legally entered transfer. *(Article 3(1), SFD)*

Protecting Against The Unwinding of Trades

Unlike in TradFi, digital asset transactions are not settled through a CSD (securities) or on a central bank ledger (cash). This means that they lack legal settlement finality, leaving settled payments vulnerable to clawbacks under insolvency proceedings. If a payment or asset transfer is later deemed "*voidable*," it can be reversed by court order, even long after the transaction was completed.

FTX vs ByBit

The prominent example of FTX's bankruptcy and the resulting dispute with the digital asset exchange ByBit exemplifies the repercussions this can have.

In November 2021, FTX's trading affiliate firm Alameda Research and ByBit executed a swap of their native tokens: 3.36m FTT for 100m BIT. Both promised not to sell for three years. When FTX collapsed a year later, **ByBit requested that the trade be unwound but FTX refused**. At this time, FTX's BIT holding was worth around $50 million, compared to ByBit's FTT value of $4 million.[12-1] However, **in the absence of a recognised settlement system with legal finality, ByBit found alternative means to frustrate FTX's rights**:

- ByBit rebranded BIT into Mantle tokens (MNT), requiring BIT holders to convert BIT into MNT to access the tokens.
- A community vote blocked FTX from converting their BIT holding into MNT.
- ByBit ultimately agreed to buyback FTX's BIT holding for nearly $53 million and release FTX's other assets.[12-2]

Despite defending against a clawback attempt, FTX attempted to enact clawbacks itself, including against the similarly bankrupt Genesis. In its lawsuit, FTX requested the return of $1.8 billion of funds from its platform that Genesis had already withdrawn. They eventually reached a $175 million settlement in late 2023, far less than the clawback request.[12-3]

FTX vs Binance

In November 2025, the FTX bankruptcy estate also sued Binance in an attempt to clawback $1.76 billion. It claimed that FTC customer funds were improperly used by Alameda Research in 2021 to finance the repurchase of Binance's large equity stakes in FTX entities. Asserting that FTX and Alameda Research were already insolvent at the time, the estate claimed that the funds were fraudulently used and should be returned to pay FTX creditors.[12-4]

Binance had three primary defences against FTX's claim:

- Insolvency protection: Binance claimed protection under the US Bankruptcy Code's 'safe harbor' provision which guards settled transactions from clawback in subsequent insolvency.
- Lawsuit filed in Delaware: Binance claimed that the three entities named were not involved in the transactions, and that the US court had no legal jurisdiction over them.
- FTX was not plausibly insolvent: Binance highlighted that FTX operated for 16 months after the sale and reached higher valuations at subsequent fundraising rounds.[12-5]

Similar to the insolvency protections afforded by settlement finality in EU and English common law, US safe harbor provisions apply to specific categories of qualified financial contracts (e.g. securities, repos). However, the buyback was funded through platform tokens FTT, BNB and BUSD, which along with other digital assets, do not benefit from the same explicit statutory protections as traditional financial instruments, **leaving their legal treatment in insolvency less certain**.

Additionally, the allegation that FTX was already insolvent opens the door for transactions made during this period to be challenged and potentially reversed. By contrast, if those transfers had taken place within formally recognised settlement system, they would be protected by settlement finality, unless the system had been notified of FTX's insolvency beforehand.

The Importance of Finality

The cryptocurrency and digital asset market is no less intertwined than TradFi, but unlike traditional finance, **clawback attempts are far more likely**. These cases illustrate the systemic vulnerabilities of operating without legally protected finality. Settlement finality laws explicitly **prevent the reversal of completed trades**, even in insolvency. The ability to unwind trades not only damages trust but also exposes counterparties to unpredictable legal risk, something robust financial market infrastructure is designed to prevent.

> *"insolvency proceedings should not have a retroactive effect on the rights and obligations of participants in a system"*
>
> *Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems*[12-6]

The Celsius Bankruptcy:

A Case Study In A Fallout Without Finality[13-1]

A Culture of Promises, Not Protections

Founded in 2017, Celsius grew into one of the world's largest cryptocurrency lending and financial platforms. Celsius positioned itself as a safer, more transparent alternative to traditional banks, promising to act in the best interest of both retail and institutional investors.

Celsius was neither a bank nor custodian, but senior leaders and company marketing consistently presented the image of a firm in strong financial health and actively claimed not to engage in risky, unsecured lending.

It **claimed to be the "*safest place for your crypto*"**, telling customers that deposits were accessible on demand, backed by billions in liquidity, and protected by a $750 million insurance policy.

In addition to crypto-based versions of traditionally familiar financial services (such as interest-bearing accounts, crypto-secured loans, and currency exchange), Celsius also aggressively marketed high-yield products. For example, its 'Earn' programme offered interest rates of up to 18.63% APY with "*no risk*" on deposited crypto. 'Earn' customers were told that their cryptoassets would remain "*yours legally*" and be "*safe forever*".

Over $4bn Frozen in Misappropriation

Customers had no visibility into how their assets were being used, nor any reason to believe that their assets were no longer their legal property once deposited.

Despite the CEO's public assurances that "*Whatever you put in, if you put in one Bitcoin you will be withdrawing one Bitcoin… It's always your Bitcoin*"; in reality, **Celsius took legal title of deposited assets, rehypothecated them into principal accounts** and used them to pay operational costs, fund rewards to other 'Earn' consumers, and invest in high-risk strategies.

Celsius lacked basic operational controls, failing to accurately track deposits and liabilities, nor maintain sufficient reserves to meet withdrawal demands. Despite this, it continued to accept new deposits while claiming to be financially stable with "*billions in liquidity*".

Unsurprisingly, customers started having trouble making withdrawals from 2020, culminating in an "existential" liquidity crisis in May 2022.

Its subsequent collapse trapped over $4.7 billion in customer assets in frozen accounts, leading Celsius to file for bankruptcy in July. 'Earn' customers **effectively had IOUs rather than their assets**.

In the absence of legal clarity, enforcement and regulatory safeguards, ownership assurances in digital asset markets can become meaningless.

When Finality Fails, Legal Chaos Follows

In the US, bankruptcy law allows for the recovery of "preferential transfers"; transfers made within 90 days of insolvency, during which the firm is presumed to have known its financial condition.

During the May-July freeze, over $20m in cryptocurrency deposits were still permitted to be made in the two weeks following the freeze on withdrawals. However, Celsius' bankruptcy administrators sought to recover $2 billion of withdrawals from around 2% of total users who withdrew at least $100,000 during those 90 days, representing 40% of the firm's assets.[13-2]

Celsius initially served settlement offers to customers to return 27.5% (later 13.75%) of the withdrawn amount. At time of publication, users that did not agree to those terms face Celsius seeking to **clawback the current value of the withdrawn cryptocurrencies plus interest and costs**. This affects over 2,000 parties around the world; trying to enforce US court judgements in other jurisdictions will have its own problems.

The Tether Dispute: Collateral Without Clarity

In the 90 days before Celsius filed for bankruptcy, Celsius borrowed Tether's USDT stablecoin, collateralised by 17,886 bitcoin (BTC). As BTC prices dropped in June 2022, Celsius declined to post the additional margin required to avoid liquidation and instructed Tether to liquidate the BTC collateral to settle its $815 million USDT position.[13-3]

In August 2024, as part of its bankruptcy proceedings, Celsius sued Tether to clawback 57,428.64 BTC (then worth $3.3 billion), alleging "*preferential and fraudulent transfers*" to protect against the impending bankruptcy, and of improperly liquidating BTC at a lower price than the market closing price. Tether denied the allegations, claiming that Celsius consented to the liquidation at the prevailing prices in line with their original agreement.[13-4]

The Takeaway: A System Without Safeguards

Celsius' high-profile collapse and subsequent legal disputes were accentuated by founder Alex Mashinsky's May 2025 sentencing to 12 years in prison for fraud and mismanagement.[13-5]

The Celsius saga clearly highlights the critical need for robust financial market infrastructure, mechanisms for settlement finality, transparency, and regulatory oversight to protect market participants from systemic risk and foster trust in the evolving digital economy.

In traditional markets, settlement finality rules explicitly cover assets and collateral held in a CSD system and protect them in case of misuse or insolvency.

In other words, the Celsius failure highlights the critical need for a CSD capable of supporting digital assets.

Safeguarding Repo & Collateral

Settlement finality is also essential to guarding against the systemic risk of unwinding posted collateral, particularly in repurchase agreements (repo), which underpin a market worth $11.9 trillion in the US in 2024 alone.[14-1]

A repo transaction involves the sale of securities with an agreement to repurchase them at a later date. These typically short-term arrangements (usually less than 24hrs) play a vital role in ensuring market stability by enabling participants to meet netted settlement obligations, manage liquidity, and execute trading strategies without liquidating positions.

The Basics of How Repo Works

Participant A has £100k cash idle on its balance sheet

Participant B needs £100k to meet a settlement obligation

Repurchase Agreement (repo)

Cash is loaned with securities posted as collateral.

Participant A receives legal title to **Participant B's** collateralised securities

Participant B receives the loaned cash from **Participant A**

Upon buying their securities back in the '*reverse repo*', **Participant B** reclaims legal title and pays **Participant A** interest on the loan, known as the *repo rate.*

If Participant B defaults during the repo period, Participant A must have legal ownership of the collateralised securities, allowing them to sell or transfer them should the borrower fail to repurchase the securities as agreed.

Crucially, **this relies on final and irrevocable legal transfer of the securities**: it must be impossible for Participant B to unwind or undo this transfer of collateral in insolvency, ensuring Participant A can recover their funds. Otherwise, Participant B, (or their insolvency administrator) could challenge the transaction, forcing an unwind and triggering wider market disruption.

To protect against this, legislation grants legal title to the cash lender for collateralised securities and ensures that collateral transfers cannot be unpicked or reversed in insolvency. **This protection is a cornerstone of systemic stability: CCPs and their members cannot operate in a regime where posted collateral is at risk of clawback.**

> *"the reduction of systemic risk requires in particular the finality of settlement and the enforceability of collateral security"*
>
> *Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems* [14-2]

Repos Still Matter in Tokenised Markets

At first glance, real-time on-chain settlement might seem to reduce the need for repos: after all, you can only trade assets you already hold. However, this assumption overlooks the reality of institutional finance.

Repos are not just about access, they are essential tools for liquidity, leverage, and risk management. Even in tokenised markets, the need for collateralised lending and margin remains. On-chain settlement does not eliminate the need for repos; it simply changes how they are executed.

Digital Assets & Collateral

As blockchain and digital markets evolve beyond peer-to-peer retail use into institutional finance, the use of digital assets as collateral is accelerating; especially through tokenised securities and smart contracts. For example:

- **Dematerialisation**: Collateralised traditional securities can be moved quickly in tokenised form, reducing settlement down from T+2 to intra-day, therefore enhancing liquidity and capital efficiency.
- **TradFi adoption of digital assets**: In 2024, the ICMA (International Capital Market Association) published a Digital Assets Annex to its Global Master Repurchase Agreement (GMRA) allowing digital cash and securities to be used in repo transactions.
- **DeFi networks**: Smart contracts automate and enforce the terms of loans collateralised with digital assets and cryptocurrencies on-chain, leveraging tokenised collateral networks to ensure transparency and efficiency. Once the loan is repaid, the smart contract releases the collateral back to the borrower.

Collateral is not solely used in repos. It is essential for meeting CCP margin requirements in leveraged trading, playing a critical role in mitigating counterparty risk. In the absence of CCPs to manage margin and CSDs to organise settlement in digital assets, many digital asset trading venues currently require 100% prefunding, locking up capital. If posted to a CCP within a recognised CSD's system, that collateral is also protected in counterparty insolvency.

The Role of the CSD

A key function of CSDs is to secure collateral through their securities settlement systems via book-entry systems. According to CSDR, collateral must be treated the same as securities traded on a regulated trading venue and must be "*recorded in a CSD book-entry system in order to ensure that all such securities can be settled in a securities settlement system.*"

By immobilising the securities and ensuring that the legal title transfer occurs within a legally recognised system, the CSD provides finality to collateral that protects market participants from the fallout of a counterparty's failure.

The Future of Finality:
How Digital CSDs Will Establish The Finality That Blockchain Alone Cannot

Despite the promise of DLT and digital assets, all technology is fallible. Developers make mistakes. Networks fail. Vulnerabilities are exploited. Black swan events happen.

Blockchain does not, and cannot, provide the legal certainty that markets require to protect against such risk and function at scale. Technology can verify; only the law can finalise.

Despite regulatory advancements, **digital asset markets remain legally ambiguous**, creating structural barriers to institutional adoption. Regulated entities cannot operate in markets where title is unclear, settlement is reversible, or legal recourse is uncertain.

In addition to key requirements such as establishing a clear moment of irrevocability, legal recognition of title and insolvency protection, there are other **critical gaps hindering institutional confidence and participation** in digital assets, including:

Unclear jurisdiction and enforcement

No single regulator can claim authority over an internationally operated decentralised platform, causing confusion as to what laws apply, how to enforce them, or how disputes can be resolved.

Inconsistent cross-border rules

Fragmented regimes and standards increase risk, complicate conflict resolution and limit scalability.

Protocol forks and unilateral changes

There is no legal mechanism or recognised authority to determine which version of a blockchain is valid when splits or changes occur.

Lack of accountability through self-governance

Usually self-governing and self-policing, decentralised systems are typically spread across jurisdictions and offshore entities with no clearly accountable executives to hold to fitness and propriety standards.

Inability to meet stress testing requirements

Financial institutions must demonstrate technical, operational and financial resilience under adverse conditions (e.g. from extreme price movements to severe economic scenarios), which most digital platforms are not yet equipped to do.

Without regulated infrastructure, digital asset markets face legal, operational, and reputational risks. Global regulatory harmonisation will take time, but market infrastructure that meets international standards can bridge the gap to deliver legal certainty, systemic protections, and trusted governance to support institutional adoption.

Finality, enforceability, and accountability come not from technology, but from legally recognised financial market infrastructure, such as central banks and CSDs. Though largely invisible to most participants, these systems are essential to contain risk, maintain market order, and prevent systemic contagion. Without them, assets are settled without finality, creating complications for courts and creditors.

To trade, custody or use assets as collateral with confidence, participants need a clear legal claim and irreversible settlement. **Technology cannot alone guarantee title transfer nor finality, so it cannot alone establish market trust**. Digital assets require both a CSD and a regulatory framework to ensure legal certainty.

CSDs: A Cornerstone of Market Trust & Provider of Settlement Finality

CSDs do far more than record ownership. They act as **synchronisation operators**, co-ordinating the simultaneous exchange of assets and central bank money: guaranteeing delivery vs payment (DvP) and enforcing settlement finality.

This enables CSDs to serve as the **single source of truth** for securities ownership, and to **define the legal "entry point" of a transaction and the moment it becomes irrevocable**, even in insolvency.

The evolution of financial technology depends on **extending the CSD framework to digital assets**. To safeguard the flow of trillions in cash and securities, **an accountable intermediary is essential for guaranteeing title transfer, the very foundation of market trust**.

Until digital asset markets are supported by legally recognised infrastructure, such as a **digital asset CSD**, they will remain fundamentally incomplete. Blockchain may offer speed, transparency, and programmability, but only law can guarantee finality.

This is why a CSD for digital assets is not just desirable, it is essential. It is the missing piece that transforms digital markets from experimental to institutional. It is the cornerstone of market integrity, the enabler of scale, and the safeguard against systemic risk.

Without it, the promise of digital assets will remain just that, a promise. With it, that promise becomes a foundation for the future of finance.

Closing the Regulatory Gap: Setting The Stage for Scalable Growth

To unlock scalable growth, digital assets need legal clarity, and regulatory standards equal to those in traditional financial markets. Without this foundation, they will remain experimental markets, unable to fully integrate into the global financial system.

When finality is guaranteed, trust follows; and with trust, digital markets can evolve from niche to systemic, unlocking their true potential. This requires updating and clarifying rules while preserving core principles: legal finality, enforceability and accountability.

Whether adapting existing legal frameworks or creating new regimes, **digital assets must be integrated into settlement systems** that ensure enforceable ownership, secure custody, reliable collateral use and protected netting.

Signs of Progress: Legislative Reform & Regulatory Sandboxes

Encouragingly, regulators beginning to close the gap. In the UK, rather than forcing innovation to fit outdated structures, authorities are rethinking how legal infrastructure can evolve to meet the demands of next-generation markets.

English common law and most financial regulation are technology agnostic. This allows innovations like DLT to be accommodated, providing that the underlying market infrastructure meets regulatory and legal standards.

Digital Securities Sandbox (DSS)

The DSS is a major regulatory innovation, offering a temporarily modified legal framework to test digital securities infrastructure. It is initially focused on settlement systems integrated with trading platforms.

Within the DSS, **digital securities depositories (DSDs) can replicate the core functions of traditional CSDs**: facilitating book entry, certifying legal title, enabling finality, and mitigating settlement and systemic risks.

By allowing live operation under tailored rules, the DSS allows regulators and participants to test new settlement models without requiring full legislative reform upfront, accelerating innovation within a legally safe environment.

This pioneering initiative aims to clarify legal treatment around ownership, finality, and oversight in digital assets: critical pillars for institutional trust and market stability.

It also allows English common law to remain technology-agnostic, evolving alongside unforeseen advancements, unlike more prescriptive approaches such as Switzerland's asset-specific rules.

More than regulatory experimentation, the DSS demonstrates a shift towards aligning technological advancement with institutional standards. **By offering a credible path to legal finality under recognised frameworks, it builds the trust needed for widespread adoption of digital assets and tokenised securities.**

Legal Foundations and Future Reforms

In parallel, the UK's Financial Services and Markets Act (FSMA) was updated in 2023 to bring "cryptoasset activities" into scope. It created new powers to develop a regulatory regime for "digital settlement assets," laying the groundwork for further reforms, such as extending book-entry rules to cryptoassets and incorporating cryptoasset clearing into the scope of UK EMIR.

The EU is also advancing its regulatory framework:

- **Markets in Crypto-Assets Regulation (MiCA):** builds on the MiFID framework, creating a unified regime for cryptoassets and securities. MiCA introduces licensing requirements for crypto-asset service providers (CASPs), mandates investor protections similar to MiFID II, and establishes disclosure standards for public offerings and trading of crypto-assets. While MiCA does not cover tokenised traditional financial instruments, it lays the groundwork for integrating crypto-assets into the broader financial system.
- **Central Securities Depositories Regulation (CSDR):** Anticipated updates to CSDR aim to support the development of digital asset settlement models, aligning post-trade infrastructure with emerging technologies.

Unlocking The Future of Finance

With these legal and regulatory advancements extending the proven CSD framework to digital assets, institutions will be able to participate with confidence, backed by the legal certainty and systemic protections that traditional financial infrastructure provides. **This is a seismic shift, allowing innovative digital finance to move from experimentation to real-world adoption.**

With legal finality in place, digital asset markets will be empowered to unlock new opportunities, from tokenisation to programmable finance.

In the final chapter of "*The Case for a Central Securities Depository for Digital Assets*", we explore how a CSD enables this future, how **ClearToken** will deliver the infrastructure to make it real and unearth the resulting benefits.

In the next chapter,

we explore how applying a CSD framework can deliver a unified market structure for tokenised securities and real-world assets, how that enables them to settle seamlessly alongside 24/7 payment infrastructure and the potential market benefits.

References

2-1: https://www.legislation.gov.uk/uksi/1999/2979/contents

3-1: https://www.bis.org/cpmi/publ/d101a.pdf

5-1: https://bitquery.io/blog/attacker-stole-807k-etc-in-ethereum-classic-51-attack

5-2: https://decrypt.co/37988/hacker-swiped-1-7-million-second-ethereum-classic-attack

5-3: https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month

5-4: https://www.coindesk.com/markets/2021/08/04/bsv-suffers-51-attack-report

5-5: https://www.fxstreet.com/cryptocurrencies/news/bitcoin-sv-suffers-51-attack-bsv-price-loses-critical-support-level-202108040427

6-1: https://coingeek.com/ethereum-classic-experiences-third-51-attack-in-august

7-1: https://eur-lex.europa.eu/eli/dir/1998/26/oj/eng

9-1: https://bitcoin.org/bitcoin.pdf

9-2: https://www.legislation.gov.uk/ukpga/2023/29

9-3: https://coingeek.com/dr-craig-wright-stolen-bitcoin-heres-what-went-down/

9-4: https://www.reedsmith.com/en/perspectives/2023/02/english-court-to-decide-extent-of-blockchain-developers

10-1: https://commonslibrary.parliament.uk/research-briefings/cbp-10305

10-2: https://bills.parliament.uk/bills/3766

10-3: https://www.legislation.gov.uk/uksi/2025/859

12-1: https://cointelegraph.com/news/ftx-files-billion-dollar-lawsuit-against-bybit-over-asset-withdrawals

12-2: https://news.bloomberglaw.com/bankruptcy-law/ftx-settles-suit-against-crypto-firm-bybit-for-228-million

12-3: https://www.reuters.com/technology/ftx-tied-alameda-gets-175-mln-claim-genesis-bankruptcy-estate-2023-08-17/

12-4: https://www.cnbc.com/2024/11/11/ftx-sues-crypto-exchange-binance-and-its-former-ceo-zhao-for-1point8-billion.html

12-5: https://fintechnews.sg/111585/crypto/binance-ftx-lawsuit

12-6: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31998L0026

13-1: https://www.ftc.gov/system/files/ftc_gov/pdf/2223137celsiusnetworkcomplaint.pdf

13-2: https://www.dlnews.com/articles/regulation/crypto-complicates-celsius-effort-to-claw-back-withdrawals/

13-3: https://tether.io/news/tether-will-defend-itself-against-shake-down-litigation-commenced-by-celsius

13-4: https://www.coindesk.com/policy/2024/08/12/tether-to-fight-celsius-33-billion-shakedown-litigation

13-5: https://www.ft.com/content/0ab6d246-d4ac-4667-8e7b-3c05ff4fb164

14-1: https://www.federalreserve.gov/econres/notes/feds-notes/the-12-trillion-u-s-repo-market-evidence-from-a-novel-panel-of-intermediaries-20250711.html

14-2: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31998L0026

About ClearToken

ClearToken is building a Central Counterparty (CCP) and settlement system to deliver robust financial market infrastructure to the digital asset ecosystem. This infrastructure will mitigate bilateral counterparty risk for settlement, financing, and derivative transactions by centralising clearing, collateral, and risk management arrangements. DvP settlement will also be achieved for digital assets. The systems will operate 24/7 to provide uninterrupted service while managing risk in real-time through margin and default fund contributions.

As a horizontal CCP coupled with the settlement system, ClearToken will facilitate the clearing and settlement of transactions from multiple venues and OTC markets globally. ClearToken intends to be multi-custodial and adhere to the highest AML and KYC standards. ClearToken's team comprises established corporate governance and financial markets professionals who share the objective of implementing the necessary framework for the digital asset market.

As a planned financial market infrastructure, ClearToken is seeking authorisation and recognition with the relevant regulatory bodies and will adhere to the IOSCO Principles for Financial Market Infrastructures together with all relevant legislation applicable to clearing houses, payment systems, securities and derivatives depositories, and also for virtual asset service providers.

For more information, please visit: https://cleartoken.io/

Contacts

Benjamin Santos-Stephens
CEO
ben@cleartoken.io

Niki Beattie
Chair
niki@cleartoken.io

Disclaimer

These materials have been prepared for information purposes only and do not constitute a financial promotion, an offer to sell or an inducement or solicitation of an offer to buy an interest in ClearToken Holdings Limited ("ClearToken").and should not be construed as such.

These materials are in summary form and have been prepared solely for informational purposes. These materials may also contain "forward-looking" statements, which can be identified by the use of forward-looking terminology such as "may," "will," "should," "expect," "anticipate," "target," "project," "estimate," "intend," "continue" or "believe," or the negatives thereof or other variations thereon or comparable terminology. Such statements are statements other than historical fact and relate to ClearToken's intent, belief or current expectations primarily with respect to its future operating, financial and strategic performance. Any such forward-looking statements, including any financial, performance or other projections, are not guarantees of future performance and may involve risks and uncertainties. Forecasted performance is subject to changes at any time and may not materialize as presented due to changes in the market or economic conditions. Actual results may differ from those contained in or implied by such statements. Neither ClearToken nor any of its directors, officers, agents or affiliates makes any representations or warranties regarding the accuracy or completeness of any projections or other forward-looking statements and assumes no responsibility to update such statements as a result of new information, future events or otherwise. Actual events, results or performance may differ materially from those reflected or contemplated by such forward-looking statements as a result of factors beyond ClearToken's control.

Forward-looking statements, including projections, included in these materials are made based on our current expectations and projections about future events and such views as they exist as of the date of publication of these materials. There is no assurance that such views are correct or will prove, with the passage of time, to be correct. Due to various risks and uncertainties, actual events or results or the actual performance of the investment may differ materially from that reflected or contemplated in these projections. Although we believe the expectations reflected in the projections are reasonable, we cannot guarantee future results, performance or achievements. Moreover, neither we nor any other person assume responsibility for the accuracy and completeness of any of these projections or have any duty to update such projections. Potential investors are cautioned not to place undue reliance on forward-looking statements.