ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Locked Out at Closing: When Crypto Fails at the Closing Table

Financial Services

Real Estate

Technology, Privacy, and eCommerce

Corporate, Securities, and Governance

Banner artwork by 3d Stock Hub / *Shutterstock.com*

Cheat Sheet

- **Understand custody risk.** Digital assets introduce unique vulnerabilities — a frozen wallet, lost private key, or custodian error can halt a closing with no traditional recovery mechanism.
- **Update contract language.** Standard purchase agreements rarely address blockchain payments, so counsel must add crypto-specific provisions such as contingencies, custody risk

allocation, and alternative payment pathways.

- **Strengthen key controls.** Because control of a private key equals control of the asset, companies need strict policies, multi-signature arrangements, and verified access procedures to prevent avoidable failures.

- **Run cross-functional checks.** Before accepting digital assets, legal must confirm access to funds, vet custodians, ensure compliance, and review insurance coverage for digital-asset risks.

A real estate investment firm is poised to close on a US$40 million acquisition. Part of the purchase is funded through a digital-asset custodian holding Bitcoin from earlier tokenized sales. Hours before the closing, the custodian freezes the account after an automated compliance flag. It is up to the legal team to determine whether the buyer has breached, whether the contingency clause applies, and how to keep the deal alive.

Scenarios like this, once unthinkable, are becoming real. While cryptocurrency still represents a small fraction of real estate transactions, its footprint is expanding rapidly. Platforms such as Propy and Figure have piloted tokenized transfers, and even luxury brokerages like Christie's now accept regulated crypto payments. According to Redfin, about one in nine first-time buyers in recent years used crypto proceeds toward a down payment. The trend is clear: digital assets are moving from novelty to negotiable instrument.

This evolution has landed directly on corporate legal desks. As investors experiment with crypto to diversify portfolios and accelerate settlement, each innovation introduces new risks: uncertain custodial responsibilities, regulatory ambiguity, and technical points of failure that traditional escrow processes never contemplated. A single lost password or frozen wallet can turn a closing into a contractual standoff involving lenders, title insurers, and compliance officers.

For corporate counsel, the binary nature of blockchain control (either you have the keys or you don't) turns a technical issue into an operational one. When value is held in code rather than cash, legal teams must anticipate failure points that originate outside the closing room. Understanding how digital-asset custody intersects with contracts, cybersecurity, and compliance is now part of standard risk management.

The following sections examine where blockchain meets real estate, why "losing the keys" can halt a multimillion-dollar closing, and what counsel can do to prevent or recover from a digital-asset breakdown.

The growing intersection of real estate and crypto

Real estate transactions have always evolved with new forms of value transfer. Today, blockchain technology and digital assets are testing how property can be bought, financed, and recorded. Though crypto-funded deals remain a small part of the market, their complexity and visibility have grown sharply.

Developers and investors are experimenting with tokenized financing structures including fractional ownership interests or profit-sharing units that trade like private securities. Luxury brokerages now list properties that can close through regulated digital-asset custodians. Each new structure blurs the boundaries among real estate law, securities regulation, and financial technology.

The promise is speed, transparency, and global reach. The challenge is that the supporting infrastructure has not caught up. Title and escrow companies, brokers, and underwriters still operate on systems designed for wire transfers and paper records. Few possess internal controls or insurance coverage tailored to digital-asset custody. As a result, legal and compliance teams often fill the gap, vetting counterparties and clarifying who bears responsibility for funds stored in wallets rather than trust accounts.

> In digital-asset transactions, the phrase "*no keys, no coin*" is more than a slogan; it's a rule of survival.

Regulatory oversight remains fragmented. The SEC continues to determine when tokenized assets qualify as securities, while FinCEN enforces anti money-laundering rules for custodians and exchangers. At the state level, money-transmitter and blockchain-recording statutes vary widely, creating inconsistent standards for market participants. Federal and state frameworks overlap unevenly, leaving in-house counsel to navigate a patchwork with limited precedent.

Real estate professionals are adopting digital assets faster than regulators or closing infrastructure can adapt. For legal departments, understanding that mismatch and the resulting operational risks is the first step toward managing them.

The unique risk of "losing the keys"

In digital-asset transactions, the phrase "*no keys, no coin*" is more than a slogan; it's a rule of survival. A private key is the sole credential granting control over a blockchain address, functioning as a unique cryptographic signature. Lose it, and access to the associated funds is permanently gone. Unlike traditional bank credentials, there is no reset function, customer support hotline, or judicial order that can regenerate a private key.

Causes range from the mundane to the catastrophic: miswritten or misplaced seed phrases, hardware wallet malfunctions, or password mismanagement by sellers or custodians. In institutional settings, access failures usually stem not from technology, but from governance lapses. Deals have collapsed because wallet credentials were controlled by one employee, scribbled on paper, or stored outside secure systems.

Avoiding these scenarios requires disciplined key management. Companies should establish policies specifying who holds, safeguards, and audits access, supported by documented recovery procedures. Unlike conventional IT credentials, cryptocurrency wallets often sit outside password vaults and identity-management systems, creating gaps that legal teams may not recognize until it's too late.

A robust key-management policy is more than a convenience document. It's a compliance artifact. It should mandate multi-signature controls, corporate backups, and board-level oversight. In crypto, operational discipline is inseparable from legal risk management.

Legal and contractual fallout

The closing was scheduled for a Friday morning. The buyer’s real-estate investment partnership planned to transfer part of the purchase price in Bitcoin from a corporate hardware wallet holding an eight-figure balance. When the wallet was retrieved from the safety-deposit box, it failed to initialize. Multiple attempts confirmed the device had been reset months earlier, wiping the private keys irreversibly.

> A “crypto contingency” can define proof of funds, establish alternative payment methods if assets become unavailable, and specify which party bears custody risk before transfer.

Fortunately, an office administrator had recorded the seed phrase years earlier, allowing restoration of access and salvaging the deal. The event exposed a deeper problem: policy and practice had diverged. Staff misunderstood how the wallet functioned and assumed the device itself stored the funds. No dual control, custody audit, or recovery test existed, leaving a single point of potential catastrophic loss.

Once digital assets enter a real-estate transaction, the legal framework governing closing risk often lags behind. Most purchase agreements and escrow instructions still assume that funds move by wire, not blockchain. When payment depends on a wallet, new questions arise: What constitutes delivery? Who bears loss if access is lost or frozen?

Few standard real-estate contracts contemplate digital-asset payments or temporary inaccessibility. If a custodian freezes funds before closing, one party may allege breach while the other claims impossibility or force majeure. Outcomes turn on how the agreement allocates risk and whether digital currency qualifies as “lawful money” or property held for exchange.

Forward-thinking drafters are starting to include crypto-specific clauses. A “crypto contingency” can define proof of funds, establish alternative payment methods if assets become unavailable, and specify which party bears custody risk before transfer. Some contracts reference escrowed stablecoins or custodial attestations to reduce volatility and exposure.

Legal teams should also ensure treasury and compliance departments can verify wallet access before signing, and confirm custodians meet FinCEN and state-licensing standards. Insurance coverage, including cyber, E&O, and title, should be reviewed to confirm it extends to digital-asset custody failures.

Ultimately, operational resilience determines whether a technical lapse becomes a legal crisis. Until model provisions emerge, clear drafting and internal verification are what prevent a lost wallet from turning into a multimillion-dollar breach.

The recovery process

When digital keys are lost at the closing table, time becomes the critical variable. The first step, before any remediation, is to establish a timeline and preserve the digital evidence trail, including system logs, device serials, and wallet addresses. From there, a forensic wallet recovery assessment determines whether the issue stems from human error, hardware failure, or cryptographic loss.

Practical recovery may involve hardware repair, chip-level data extraction, or device re-initialization when memory remains intact. In some cases, partial seed reconstruction is possible using fragments, backups, or derivation paths. For institutional clients, cross-referencing offline address databases can confirm ownership and transaction history, providing proof for insurers or auditors.

Counsel should coordinate immediately with forensic experts, custodians, and insurers to document the loss event. Thorough documentation is essential if recovery fails and the matter escalates to litigation or insurance claims. From a legal perspective, such incidents should be treated as both operational and regulatory events. Immediate notice to insurers, custodians, and, where applicable, FinCEN-registered entities preserves coverage and compliance defenses.

It’s important to dispel myths: true cryptographic loss is irreversible, but many “lost” wallets result from preventable operational failures. Acting quickly and documenting properly can mean the difference between an interrupted closing and a permanent asset impairment.

> Digital assets are not going away. The in-house lawyers who understand both the technology and its legal implications will be the ones guiding their organizations through the next generation of real estate transactions without losing control of the keys.

Preventative measures for real estate and legal teams

Crypto-related closings most often fail not because of technology, but because of inadequate preparation. Before any contract involving digital assets is executed, both legal and technical teams must verify proof of access to those assets. A wallet screenshot is not enough; the counterparty should demonstrate control through a signed transaction or verification message.

Multi-signature escrow arrangements remain the most effective safeguard. They distribute control across independent parties (typically a buyer, seller, and escrow agent) which mitigates a single-point-of-failure risk. Custodians should meet basic standards such as SOC 2 compliance, use of hardware security modules (HSMs), and cyber-insurance coverage.

Due diligence should also include KYC/AML verification, review of key-management procedures, and confirmation that backup methods align with corporate data-protection policies. Insurance coverage often lags behind these technical realities, so counsel should confirm that E&O, cyber, and title policies explicitly address digital-asset custody and transaction failures.

A concise due-diligence checklist helps legal and closing teams reduce risk before accepting crypto in any transaction:

- Proof of access to funds before contract execution.
- Multi-signature escrow arrangements preventing unilateral control.
- KYC/AML verification for custodians and transacting parties.
- Insurance coverage addressing wallet management and key storage.

Training is equally vital. Brokers, escrow officers, and in-house staff should understand wallet access, transaction timing, and blockchain verification. Tabletop exercises can expose policy gaps before they cause loss.

Finally, legal professionals should vet custodians and escrow providers for licensing, cybersecurity

posture, and insurance — the digital equivalent of confirming that trust funds are properly safeguarded. These steps reduce liability and maintain confidence as the industry adapts to new forms of value transfer.

Role of in-house counsel and closing takeaways

For in-house counsel, the rise of crypto in real estate brings both opportunity and exposure. Legal teams operate where innovation meets compliance, and even small policy gaps can become financial risks. Counsel's responsibility extends beyond drafting purchase agreements. It includes establishing internal protocols for digital-asset custody, vetting custodians, and updating contract templates to reflect alternative payment methods and contingency plans.

Cross-functional coordination is essential. Legal, compliance, IT, and finance must communicate early to confirm access verification, regulatory coverage, and documentation standards before crypto ever enters the closing process.

A short readiness checklist helps keep deals on track: confirm proof of access to funds, include crypto-contingency language, verify insurance coverage, and define communication channels if a transaction stalls.

Digital assets are not going away. The in-house lawyers who understand both the technology and its legal implications will be the ones guiding their organizations through the next generation of real estate transactions without losing control of the keys.

Join ACC for more in-house insights!

Debbie Hoffman

Visiting Assistant Professor of Law

Cleveland State University College of Law

Debbie Hoffman is a Visiting Assistant Professor of Law at Cleveland State University College of Law and a former General Counsel in the financial services and technology sectors. She previously founded Symmetry Blockchain Advisors and serves on several corporate and nonprofit boards. Her work focuses on digital assets, innovation, and emerging legal issues.

Wesley Brandi

CTO

Praefortis

Wesley Brandi, PhD, is the CTO of Praefortis, a crypto hardware wallet recovery and digital forensics firm, and has spent more than two decades investigating complex online fraud and abuse for clients including Microsoft, Apple and US government agencies. He previously led a covert threat-mitigation team at Amazon, and has published peer-reviewed research on affiliate fraud, click-fraud detection, and online privacy.