

RWA CASE STUDY · OCTOBER 2026

Issuing a Security Token Is Easy. What Happens Next?

*The Real-World Challenges of Operating a Regulated Tokenised
Securities Marketplace*

THE FIRST QUESTION

“I’ve lost my private key. Have I lost my \$250,000 investment?”

FOR OPERATORS OF REGULATED RWA MARKETPLACES

WHAT SHOULD THE MARKET BE ABLE TO DO BEFORE THE FIRST TOKEN IS ISSUED?

THE SCENARIO

A Call to Customer Services

The call comes through to customer services. An investor says they cannot access the wallet containing \$250,000 of tokenised securities. The tokens appear to be on the blockchain. But can the investor still exercise the rights they paid for?

It is a simple, human question with a complicated answer. It touches legal ownership, private-key control, record keeping, customer asset protection and the marketplace's ability to put things right.

Now imagine the marketplace has not yet launched. A client is planning to establish a regulated RWA venue and asks Hogswood to think through the questions that will arrive from investors, issuers, internal teams, auditors and competent authorities.

What should the market be able to do before the first token is issued?

The following calls and enquiries are fictional, but the operational issues are real. The purpose is not to prescribe a blockchain or write code. It is to identify the outcomes that the legal, regulatory, operational and technology arrangements must deliver together.

THE CASE AT A GLANCE

THE CALL

An investor cannot access a wallet holding \$250,000 of tokenised securities

THE SETTING

A regulated RWA venue that has not yet launched

THE ASKERS

Investors, issuers, internal teams, auditors and competent authorities

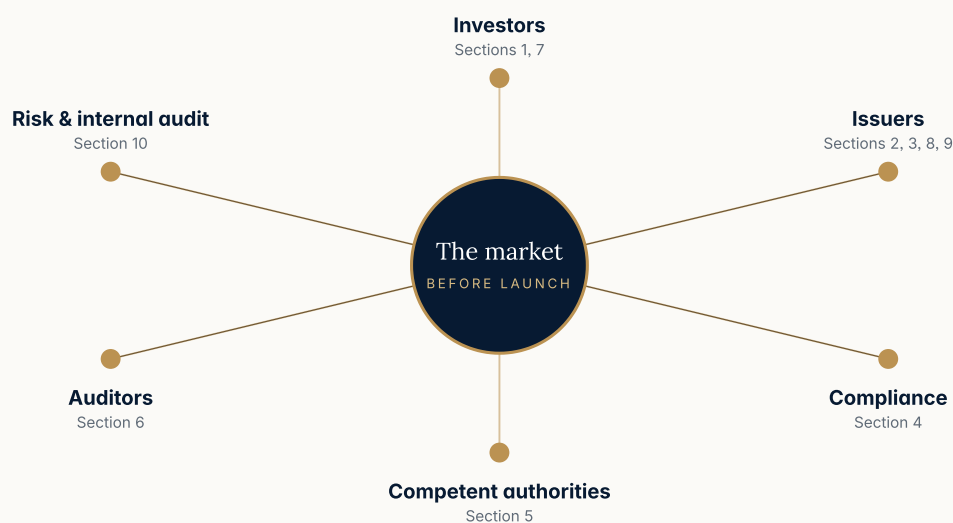
THE PURPOSE

To identify the outcomes the legal, regulatory, operational and technology arrangements must deliver together

NOT THE PURPOSE

To prescribe a blockchain or write code

FIGURE Who will be asking — the questions arrive from every direction



THE INVESTOR

01 “I cannot access my securities.”

THE CALL

“I’ve lost my private key. Does that mean I have lost my investment?”

The blockchain may still show the tokens in the original wallet. Yet the investor can no longer authorise a transfer. If the token were an unrestricted crypto-asset, permanent loss of access might be part of the model. A regulated security raises a different question: has the investor lost the security itself, or merely a means of controlling its digital representation?

The operator first needs to establish identity and legal entitlement, then determine whether a key was lost, stolen or otherwise compromised. It must also understand who is responsible for the wallet and custody arrangement: the investor, a nominee, a custodian or another service provider.

Depending on the law and structure, recovery might involve restricting an inaccessible wallet, updating an authoritative record, reassigning a holding or replacing tokens under controlled procedures. Whatever the method, the operator must avoid creating two valid claims to one security. A legitimate investor should not be left without an available route to establish and, where the framework permits, restore access to their rights merely because a credential has failed.

This is customer asset protection as well as customer service. It is the kind of issue that can damage confidence in a market long before anyone asks how quickly its blockchain settles.

OPERATOR’S DESIGN QUESTION

How will a verified investor recover access while preventing duplicate holdings or fraudulent recovery?

THE ISSUER

02 “Who actually owns the tokenised security?”

THE CALL

“Is the person who controls the wallet automatically the owner?”

This takes us back to a familiar securities distinction. Historically, some instruments were issued in bearer form: possession of the instrument was central to exercising or transferring its rights. Registered instruments operate differently. A legally recognised register or record, rather than mere possession of a certificate, establishes ownership in accordance with the applicable law.

Restrictions on bearer instruments were not simply a preference of securities operators. In many jurisdictions they followed legal, regulatory and public-policy measures intended to improve ownership transparency and address money laundering, terrorist financing, tax evasion and related risks. Approaches differ: bearer securities may be prohibited, immobilised or subject to special controls.

Now consider a token that can move freely between pseudonymous wallet addresses. This does not make that token legally a bearer security. But the design can create bearer-like operational characteristics when control of a private key effectively determines who can move the asset, without an authoritative link to the person legally entitled to the underlying security.

A blockchain records which address holds a token. That is not necessarily the complete answer to who owns the security. A custodian might control the address for a client. The issuer might maintain a separate register. In some frameworks a distributed ledger itself may constitute all or part of the legally recognised register; in others it may not. The documents, legal framework and operating model need to settle that question.

If the on-chain and legally authoritative records are different, the operator must know which controls keep them aligned and what happens when they disagree. Digital portability should not inadvertently recreate the transparency and ownership problems that securities law sought to address.

OPERATOR'S DESIGN QUESTION

What is the authoritative ownership record, and how are the security, token and legally entitled holder connected?

THE ISSUER

03 “Can these tokens go to the wrong investor?”

THE CALL

“We issued to approved investors. What stops one of them sending tokens to somebody else?”

Wallet A proposes to send 1,000 security tokens to Wallet B. The signature may be cryptographically valid. Yet Wallet B might belong to an unknown recipient, an investor in an excluded jurisdiction, or someone who does not qualify under the security's offering conditions.

Identifying an investor is only half the task. Eligibility may depend on investor category, beneficial ownership, residence, transfer restrictions, minimum holding conditions or other requirements attached to that particular instrument. Eligibility can change after onboarding: a company's beneficial owner changes, an investor relocates, a holding period expires or a restriction is imposed.

An operator therefore needs an ongoing link between verified identity, associated wallets and the securities that person is permitted to acquire or hold. A token that can be transferred outside the platform's web interface must still be subject to the applicable controls. Otherwise, an apparently compliant trading screen may mask

uncontrolled wallet-to-wallet transfers.

The solution could combine approved addresses, pre-transfer checks, registrar permissions, custody controls and token-level restrictions. The design choice belongs to the legal and technology workstreams, but the outcome is clear: a technically possible transfer should not automatically become a permissible transfer.

OPERATOR'S DESIGN QUESTION

Can the market prevent or properly resolve an impermissible transfer, including a direct wallet transfer outside its interface?

COMPLIANCE

04 “Our screening system has flagged an investor.”

THE CALL

“We have a possible sanctions match. The client is trying to move their holdings. What happens now?”

A potential match requires investigation; it should not automatically be treated as a confirmed designation. Compliance needs to assess the match, identify the applicable obligations, escalate where appropriate and determine whether a freeze, transfer restriction, reporting or another measure is required.

That decision needs a route into the technology and operating model. Who identifies the relevant wallets and securities? Can transfers be stopped promptly? Can payments or distributions be handled in accordance with any restrictions? Can controls be adjusted or released if the alert proves false or the legal position changes?

Blockchain immutability does not require the legal position to be frozen in time. The original transaction history can remain intact while future movements of a holding are lawfully restricted. The important safeguards are speed, proportionate intervention, authorisation and an auditable explanation of what occurred.

OPERATOR'S DESIGN QUESTION

Can compliance investigate, restrict, report and subsequently release controls where legally appropriate?

THE COMPETENT AUTHORITY

05 “We require action on this holding.”

THE CALL

“A court order affects these securities. Can you give effect to it and preserve the records?”

The operator must first establish the authenticity, scope and legal effect of the direction. A regulator’s enquiry, a court order and a law-enforcement request are not interchangeable; the authority to act and any reporting obligations depend on the circumstances.

Where an intervention is required, the marketplace needs to understand which entity can act. It might be the operator, custodian, registrar, issuer or a combination. The mechanism could restrict transfers, preserve holdings and records, or support a legally directed change. It should leave a record of who requested, authorised and executed the action.

That is not a case for giving one administrator an unrestricted “master key”. It is a case for narrowly defined powers that can be exercised with proper checks when the law requires them.

OPERATOR’S DESIGN QUESTION

Can the responsible parties implement lawful directions without compromising the transaction history or overriding investor safeguards arbitrarily?

THE AUDITOR

06 “Can you prove who holds the securities?”

THE CALL

“Our client says it owns these tokens. What independent evidence can you provide?”

An authorised auditor may be acting for an individual investor, fund or company. An issuer’s auditor may instead be asking whether the number of outstanding tokens matches the securities legally issued. These are different questions, and a blockchain balance alone may not answer either.

A wallet address shows where tokens are recorded. It does not necessarily prove the identity of the beneficial owner, the legal title of the holder, who has access to the private key or whether a custodian controls the asset on another person’s behalf. Control of a key and legal entitlement should not be treated as interchangeable audit

assertions.

Depending on the arrangements, useful evidence may include investor due-diligence records, wallet-to-client mapping, register or nominee records, custody confirmations, transaction history, segregation arrangements, access-control evidence and reconciliations. The operator should distinguish facts it can independently confirm from records maintained by issuers, registrars or custodians, and protect client confidentiality.

The issuer's auditor asks a second question: one million securities were legally issued, but the blockchain appears to show 1,000,100 active tokens. Why? It may be a mapping error, a failed cancellation, an unauthorised mint or something else. The exact cause is not the point: the marketplace needs controls to identify the discrepancy, stop it being ignored, investigate it and reconcile authoritative records, token supply and any custody or payment systems.

An audit trail must also explain exceptional events: a restricted transfer, recovery following a lost key, a changed entitlement, a token burn or a corrected record. An immutable chain can provide strong evidence of recorded transactions, but an auditor still needs to understand their legal and operational meaning.

OPERATOR'S DESIGN QUESTION

Can authorised assurance providers verify existence, rights, control and completeness—and can the operator explain and resolve record mismatches?

THE INVESTOR OR FAMILY REPRESENTATIVE

07 “What happens when control or entitlement changes?”

THE CALL

“My key was stolen.”

“I have inherited these securities. How do I access them?”

“The company holding the securities has been dissolved.”

These are different events and cannot be solved by the same button. A stolen or compromised key calls for incident response, evidence preservation, attempts to contain further loss and an assessment of whether any completed transfer can lawfully be challenged or remedied. On-chain transfer finality and legal ownership may produce difficult questions; recovery is not always automatic or guaranteed.

Inheritance or a change in an investor's legal capacity raises questions of succession and representation. The operator needs to know what evidence establishes an executor's or representative's authority, whether a beneficiary qualifies to receive the instrument and how the register and token records should be updated. Insolvency or corporate dissolution may involve a liquidator or another legally authorised party.

In each case the market should have a defined route to the appropriate responsible person, with identity checks, legal review, safeguards against fraud and a complete audit trail. The goal is not to erase a legitimate past transaction but to manage the rights that exist today.

OPERATOR'S DESIGN QUESTION

Can the market respond when private-key control and legal entitlement diverge, without compromising other investors?

THE ISSUER

08 “Who receives the coupon—and who can vote?”

THE CALL

“The bond pays interest next week. A holder sold yesterday. Who gets paid?”

Issuance and trading are only part of the life of a security. Consider a five-year debt instrument with periodic coupons. The operator, registrar and payment agent must know the relevant record date, which person is entitled to payment under the instrument, and how a transfer immediately before that date affects the answer.

The answer may depend on contractual terms, settlement arrangements and the legally recognised register. Payment could be automated, processed through an external agent or handled in another way. In all cases, on-chain balances, entitlement records and payment instructions should remain consistent. There may also be restrictions on paying particular holders.

Now the issuer wants investors to approve a change in the bond terms. Can the appropriate holders be identified and contacted? How are consent thresholds calculated? Can a vote be recorded and connected to the person legally entitled to cast it? What changes in the systems when the amendment becomes effective?

Equity raises similar questions, often without a maturity date: dividends, voting, share splits, consolidations, repurchases, class changes, mergers and liquidation. Defaults and restructurings can also alter a debt holder's rights. Tokenisation does not make these conventional securities events disappear; it creates an opportunity to administer them more effectively if the design anticipates them.

OPERATOR'S DESIGN QUESTION

Will the token and supporting records continue to reflect payment, governance and corporate-action rights throughout the security's life?

THE ISSUER

09 “The bond has matured. Why are the tokens still circulating?”

THE CALL

“We repaid investors last month. Someone has just asked whether they can buy one of the old tokens.”

This is a particularly revealing lifecycle problem. If a five-year bond is repaid in full and the obligations represented by its tokens have been discharged, the marketplace should not leave apparently live, transferable tokens sitting in wallets indefinitely. A buyer should not discover years later that the token they acquired represented a debt already settled long ago.

The appropriate process might be redemption followed by burning, cancellation, recall, disabling of transfer or another legally supported mechanism. Token supply and authoritative records should reconcile after the event. The history of issuance, ownership and repayment should survive; the ability to circulate a security that no longer exists should not.

There is an important distinction: reaching a contractual maturity date is not the same as being repaid. If a bond matures but the issuer defaults, investor claims may remain outstanding. The operator must not destroy or misrepresent those claims simply because a calendar date has passed. Cancellation should follow the legal effect of the event and verified discharge of the relevant rights.

Shares require a different lifecycle model. Ordinary equity can remain in issue indefinitely. But a split, consolidation, repurchase, merger, exchange or liquidation may require existing units to be adjusted, cancelled or replaced. The system must support those events without creating duplicates or leaving obsolete tokens able to circulate as current shares.

OPERATOR'S DESIGN QUESTION

What ends the token's active life, who authorises it, and how is the legal event proved before tokens are cancelled or disabled?

RISK AND INTERNAL AUDIT

10 “Who is allowed to intervene?”

THE CALL

“Someone can freeze or reissue tokens. Who approved that power, and who checks its use?”

Recovery, freezes, forced restrictions, reissuance and token cancellation are necessary capabilities in some market structures. They also create concentrated operational risks. If one employee can freeze a holding, transfer it to a new address and conceal the action from internal records or oversight, the control framework has a problem.

The first line of defence operates day-to-day processes and owns their risks. Risk management and compliance typically provide second-line oversight and challenge. Internal audit independently tests whether the arrangements are designed and operating effectively as a third line. Actual responsibilities depend on the regulated firm’s governance and outsourced arrangements.

Different powers need different safeguards: role-based authority, segregation of duties, dual control or multi-party approval, secure signing-key arrangements, documented reasons, logging, periodic access reviews and independent checks. A routine coupon payment may be automated. Probate recovery or a court-directed restriction may require substantive human judgment. Governance is not an obstacle added after coding: it is part of what makes a capability acceptable in a regulated environment.

OPERATOR’S DESIGN QUESTION

Can the operator explain who may act, under what authority, with whose approval and with what independent oversight?

PUTTING IT TOGETHER

11 A five-year security: testing the whole operating model

The individual questions are connected. Consider a single fictional five-year tokenised debt security admitted to the proposed marketplace:

FIGURE One fictional five-year tokenised debt security, tested end to end



AT ISSUANCE

Investors are verified, eligibility checked, the security admitted and the relationship between tokens issued and legal rights documented.

YEAR 1 Transfer

Investor A transfers a portion to Investor B only after the applicable recipient and instrument restrictions are satisfied.

YEAR 2 Recovery

Investor B loses a key. Verified entitlement is restored through a controlled process without duplicating outstanding securities.

YEAR 3 Sanctions

Compliance identifies a confirmed applicable restriction on another holder and gives effect to it while preserving transaction history.

YEAR 4 Amendment

The issuer obtains any necessary holder consent and the updated rights are reflected across authoritative records and the digital representation.

YEAR 5 Conclusion

A valid final payment is made and, once rights are discharged, the related tokens are redeemed or disabled; if unpaid, the claim is not silently extinguished.

At each point an operator, issuer, investor, compliance officer or auditor may need evidence of what happened. That is what the control framework is for. It is also why token selection cannot be the first and only design decision.

QUICK REFERENCE

The operator's desk: problem-to-response guide

A quick reference to the scenarios and the corresponding design considerations. Section references relate to this case study.

WHO ASKS / WHAT GOES WRONG	WHAT THE OPERATOR NEEDS TO ADDRESS	SEE
Investor: lost key	Verify legal entitlement; provide governed recovery and prevent duplicate claims.	1
Issuer: who owns it?	Identify the legal record and reconcile on-chain control with recognised title.	2
Issuer: transfer to wrong recipient	Apply ongoing investor eligibility and security-specific transfer restrictions.	3
Compliance: sanctions alert	Investigate, restrict, report and release controls when appropriate.	4
Authority: court or regulatory action	Validate legal authority; apply controlled intervention and preserve evidence.	5
Auditor: prove the holding	Provide defensible evidence of identity, rights, custody and key control.	6
Auditor: token supply mismatch	Reconcile outstanding securities, active tokens and related records.	6
Investor: stolen private key	Contain risk; investigate and consider available lawful remedies.	7
Inheritance or incapacity	Verify lawful representation and entitlement before reassigning holdings.	7
Issuer: coupon or dividend	Establish entitled holders and reconcile payment instructions.	8
Issuer: votes, changes or default	Support notices, voting, amendments and changed investor rights.	8
Issuer: repaid bond still active	Redeem, cancel, burn or disable the token following verified discharge.	9
Issuer: split, merger or liquidation	Update, replace or cancel units in line with the legal security event.	9
Risk and internal audit: intervention powers	Define authority, segregation, approvals, logging and three-lines oversight.	10
Operator: end-to-end readiness	Test every control together across a security's full lifecycle.	11

READINESS

Before the first token is issued

For the client establishing a regulated RWA marketplace, the important question is not “Which token standard should we use?” in isolation. It is whether the intended market can identify and protect the investor, administer the security, comply with lawful restrictions, evidence its records and deal with the events that no one hopes will occur.

Those outcomes may be delivered partly by smart contracts and partly by the issuer, registrar, custodian, transfer agent, operator or other service providers. The allocation depends on the security, the applicable law and the chosen market structure. Hogswood’s task at this stage is to bring those legal, operational and regulatory questions into the design brief before permissions are sought, rather than discover them after launch.

THE CLOSING THOUGHT

A tokenised security should do more than move successfully between wallets. It should remain a trustworthy representation of the underlying legal rights when real life intervenes.

THE FIRM

About Hogswood

Hogswood is an independent advisory practice led by Adrian Hogg FCA, drawing on more than 25 years in financial services and investment business, including a decade in blockchain, digital assets and real-world asset lifecycles – with exchange, licensing and regulatory experience in the United States, Singapore, Gibraltar, El Salvador, Labuan (Malaysia), Estonia and Cagayan (Philippines).

Adrian Hogg FCA

FOUNDER

Regulated Markets · Digital
Assets · RWA Lifecycles**adrian@hogswood.group**
hogswood.group

OCTOBER 2026

REAL ASSETS. REGULATED MARKETS. REAL OUTCOMES.

Start a conversation

Independent specialist advisory and implementation support.

THE RWA LIFECYCLE

**adrian@hogswood.group**
hogswood.groupRegulated Markets · Digital Assets · RWA
Lifecycles

IMPORTANT NOTICE

The calls, enquiries and scenarios in this case study are fictional. They are intended to illustrate the legal, regulatory, operational and technology questions a regulated RWA marketplace operator should consider before launch. This case study is for general information only and does not constitute legal, regulatory, investment or other advice. The position in any real case depends on the applicable law, the security concerned and the chosen market structure.