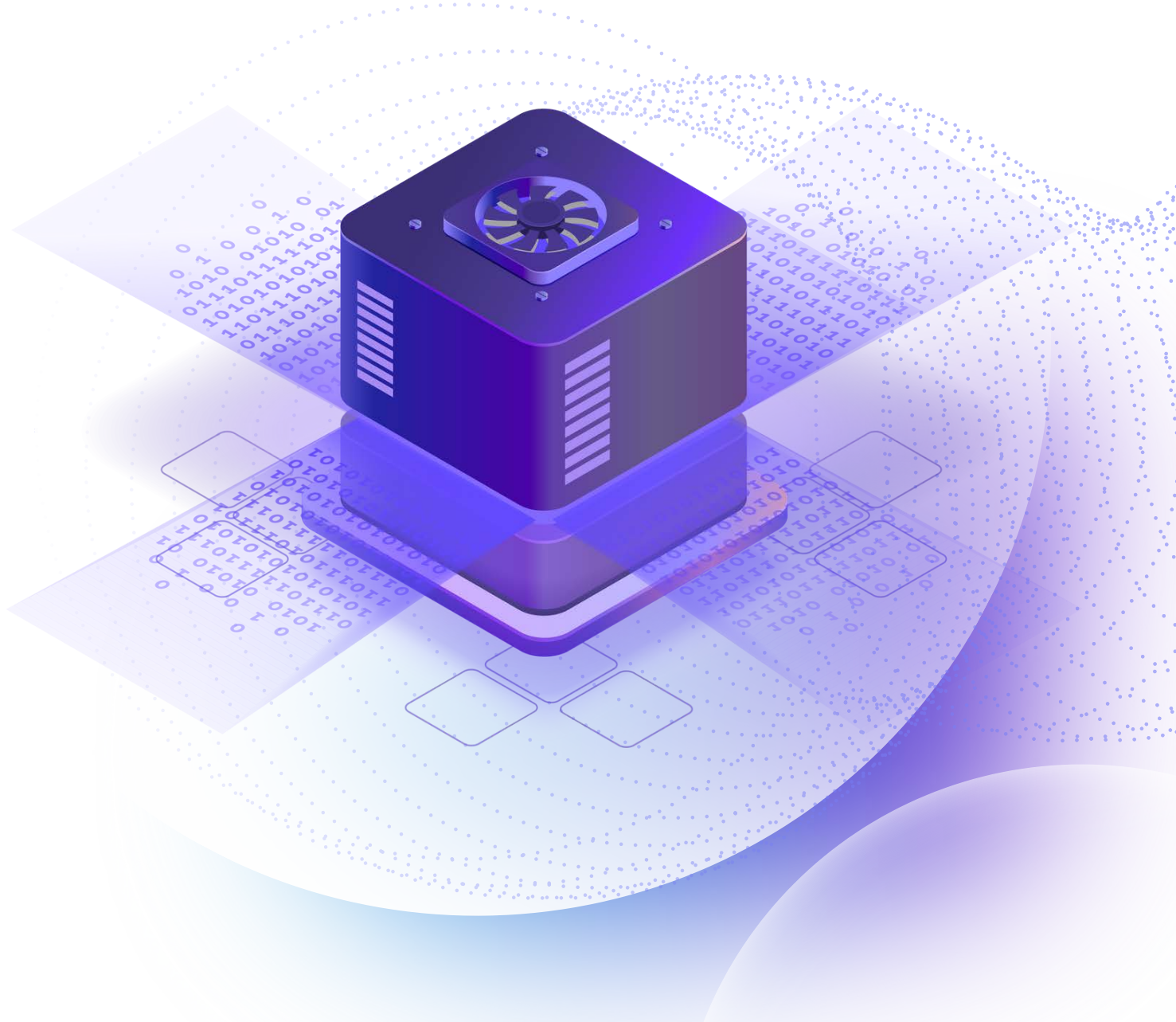


OASIS PRO

How Tokenized Securities are Evolving the Financial Industry

A three-part series explaining how security tokens work and the steps that financial institutions should take to capitalize on the benefits.



By:

Walker McKeough, Senior Associate

Jillian Wollman, Head of Marketing & Communications

PART 2

Platforms and Tools for Securities Tokenization

In the second part of our series about how tokenized securities are evolving the financial industry, we examine the technology, processes, and people needed to take advantage of this digital evolution.

Wherever you look, traditional banking systems are being upgraded with digital technology. Mobile/online banking platforms, for example, have become the standard for clients across both commercial and retail sectors.

The capital markets sector, until recently, has lagged behind their banking counterparts. But this is set to change with the arrival of distributed ledger/blockchain technology, which has the potential to accelerate the digitization of the securities industry.

The tokenization of securities will be key, enabling institutions and investors to take advantage of instantaneous settlement, intra-day liquidity, and streamlined process flows. In this article, we will guide you through the platforms and tools that open the door to these benefits, including governance structures, network security mechanisms, and smart contract standards.

Decentralized Governance

While traditional payment networks and asset transfers rely on a single entity to maintain a record of transactions, blockchain networks are decentralized and distribute responsibility for validating and recording transactions across multiple parties. This has a profound impact on the governance model of security tokens.



Single party control over an asset requires everyone who interacts with that party to trust and rely on that party's systems. By contrast, blockchain networks enable multiple parties to interact directly, without a trusted intermediary. You can even compare this with the difference between centralized and federalized governments, where power sharing with local authorities still requires guardrails and norms for maintaining order. In the same way, security token governance depends on several factors including networks where the asset is issued, as well as the business logic encoded in the smart contracts.

Public vs. Private Blockchains

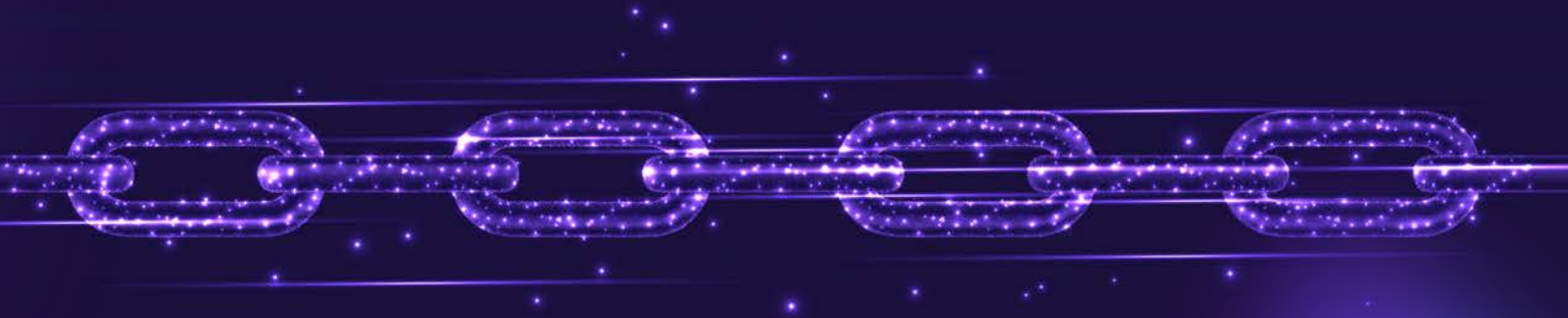
Token issuers must think carefully about where to issue their tokens and the impact of the chosen network on a token's technical capabilities, accessibility, and governance. Although it can be challenging to issue tokens over multiple networks, a range of solutions are being developed that support interoperability. On top of technical engineering requirements, institutions should apply regular thirdparty risk management (TPRM) and vendor selection frameworks when making this decision.

Public blockchains are "permissionless" in that they allow any user to join and participate in the activities of the blockchain network. They provide a truly decentralized space where all data is transparent and immutable. Any public actor who meets the qualifications is eligible to run their own node, or store transaction records, and function as a validator. Thus, public blockchains benefit from large ecosystems, leading to greater interoperability, more streamlined tooling, and greater transparency for documentation.

The potential drawback is a notable reduction in security and investor privacy that may be unacceptable for institutional asset managers and other regulated participants. Decision makers should also keep in mind that node operators controlling these networks may be based in foreign and sensitive countries. For example, participants in China exercise significant control over the Bitcoin network thanks to their involvement in Bitcoin mining ventures.

On the other hand, private blockchains may contain more sophisticated privacy features whereby only authorized parties are permitted to participate in the network. These networks may be run by a consortium of businesses, or even by a single organization that wants to manage transactions between its subsidiaries.

Whereas in public blockchains each participant has the same access and control over the network, private blockchains can incorporate roles and permissions that vary between users. This makes it easier to roll back transactions or address errors if a quorum of participants agree. For example, a regulator may be able to view transactions for auditing purposes, but not create transactions themselves. These characteristics may make private blockchains more appealing for the issuance of tokenized securities.



Smart Contracts

Smart contracts are pieces of code published to the blockchain network that can execute functions consistently across all participants, similar to formulas in a spreadsheet that automate certain tasks. This enables smart contracts to facilitate disbursements and other back-office functions.

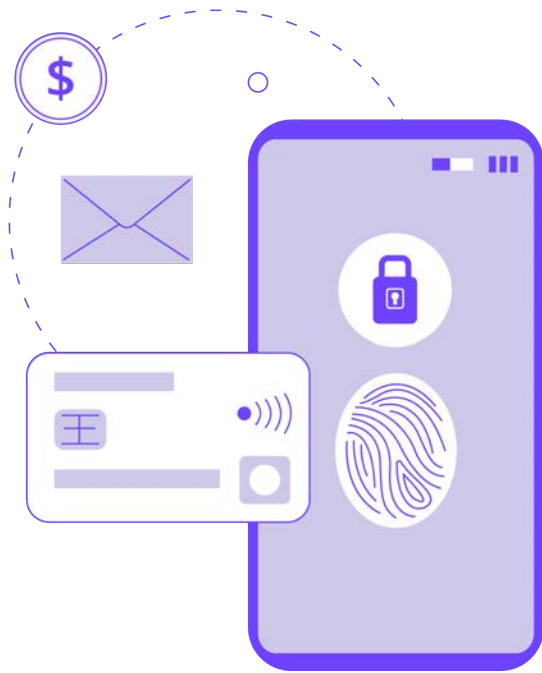
From a structural standpoint, smart contracts typically consist of multiple functions. These dictate how external applications can interact with the contract. For example, a smart contract for a cryptocurrency might contain a function called “mint” that issues new tokens. Within the mint function, the contract could stipulate who can call the function, as well as the logic which ensures that the maximum supply of tokens is not exceeded. A security token contract might also have a function called “mint,” but this may also include issuance rules such as verifying that the recipient is a whitelisted address associated with an accredited investor.

This kind of functional overlap across multiple assets can be intentional, aiming to unlock a wealth of benefits for various stakeholders. Many blockchain networks now have improved leveraging standards that specify certain names and arguments for functions. Ethereum’s “Ethereum Request for Comments” (ERC) standards have been used to create assets that are highly interoperable, for example. As a result, these assets are easier to integrate with exchanges and other applications.

Today, most cryptocurrencies are based on the ERC-20 standard, but there are multiple other standards in development for tokenized securities. ERC-3643 recently achieved ‘final’ status and thus became the token standard for real world asset tokenization and ERC-1400 has been proposed by Ethereum token issuance platform Polymath. Both include additional functions which address regulatory requirements and issues specific to security tokens.

So, while smart contracts are used to govern both security tokens and most cryptocurrencies, the logic they contain differs enormously. For example, ERC-20 tokens typically include a single transfer function that moves funds from the holder to the receiver, whereas security token standards may have a forced transfer function that enables the token issuer or some other authorized third-party to force a transfer of funds between parties—even if the holder does not initiate or agree to the transfer. Security tokens can also contain additional transfer restrictions that impose automated KYC/AML checks before allowing funds to be transferred. Such restrictions would be objectionable to cryptocurrency users but are necessary and beneficial for tokenized securities.

However, ERC standards only prescribe the function names and arguments, not the actual implementation or underlying code. If an issuer were to claim that a contract complies with a particular standard, that does not necessarily make the contract trustworthy. An audit must also be conducted on the underlying code in the smart contract to eliminate any vulnerabilities. Bear in mind that blockchain ledgers are transparent and immutable so the contract can be verified against the version that underwent the audit.



Innovation Through Implementation

By encoding the logic of security transactions and back-office processes into smart contracts that are housed on a blockchain, capital market participants can reap the benefits of their digital transformation strategies by automating manual processes and repetitive, paper intensive, back-office functions. Traditionally illiquid private assets can be traded between parties. Repo and reverse repo transactions can be settled instantaneously. Liquidity can be provided for assets on the same day instead of a multiday timeframe. These innovations enable firms to work their cash and investments faster and find innovative new ways to generate yield.

In the third and final part of this series, we will look at the steps that institutions and investors can take to unlock the potential of security tokens.

Find out more about how to take full advantage of digital securities and tokenization:



www.oasispro.com



info@oasispromarkets.com.