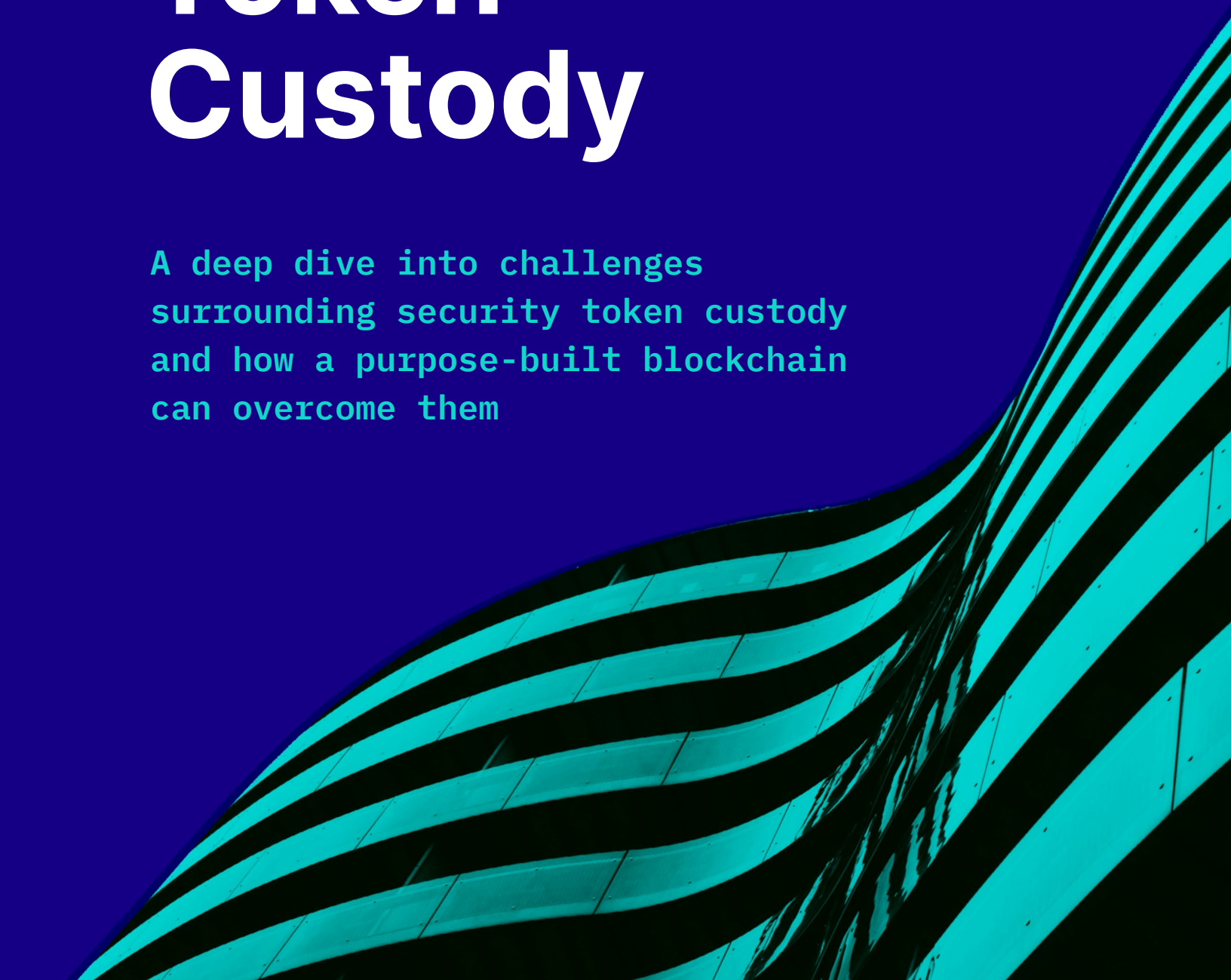
POLYMATH™

Security Token Custody

A deep dive into challenges surrounding security token custody and how a purpose-built blockchain can overcome them



This document is prepared by Polymath to show how custodians can use Polymath technology and the Polymesh blockchain.

This document does not constitute, nor shall it be construed as, a recommendation or an offer or solicitation to sell or acquire any security or investment in any jurisdiction including any investment in or purchase of securities of PingAsset. Polymath is not a broker-dealer, investment advisor or financial advisor and is not registered with any regulatory agency or body and does not provide any investment or legal advice, endorsements, analysis or recommendations with respect to any securities or assets.

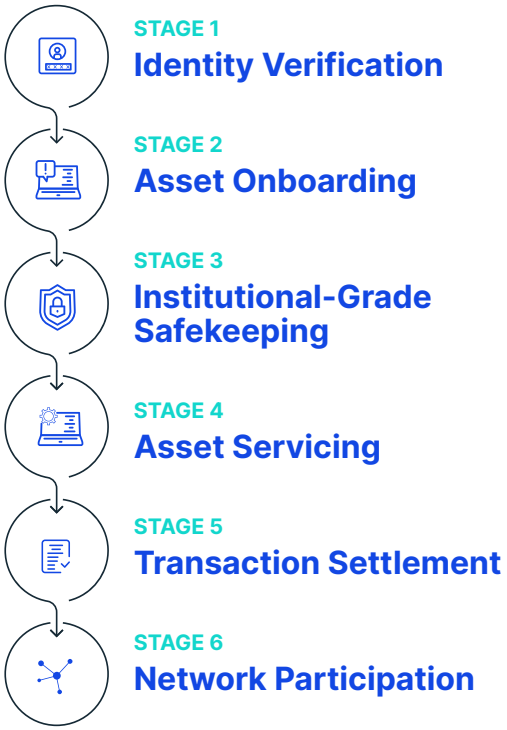
The information in this document does not purport to be complete and has not been independently verified. Polymath gives no undertaking, and is under no obligation, to update this document or provide any additional information or to correct any inaccuracies which may become apparent.

Executive Summary

The global custody market is expected to reach $34.6 billion by 2023 and digital assets are becoming an increasingly large slice of the pie. Security tokens, which are digital representations of regulated assets, come with a unique set of requirements. While they are intended to bring efficiency and automation to capital markets, digital asset custodians often face scalability and efficiency issues when handling them on public blockchains.

Initially, it seemed that security token architecture simply needed to be standardized. In time, it became clear that the challenges were more deeply ingrained and that while Ethereum is suitable for many purposes, it has gaps in functionality that prevent custodians from efficiently and compliantly managing security tokens.

Security tokens have specific requirements around identity, compliance, confidentiality, and governance that can't be met on Ethereum in a scalable and cost-effective way. By contrast, a purpose-built blockchain can solve problems with public infrastructure through key design principles built into the base layer of the chain, thereby giving digital asset custodians a better way to manage every phase of the security token lifecycle.



The evolving role of the digital asset custodian

According to Deloitte[1], there are five key reasons why digital asset custodians are becoming increasingly important to issuers, investors, and the broader digital securities ecosystem.

1. Reduced risk and complication
2. Increased security
3. Recourse for investors
4. Safer than exchanges
5. Operational efficiency

[1]Source.

Two challenges with security token custody

CHALLENGE #1

Lack of Standardization

Most tokens, even to this day, are based on the ERC 20 standard, which was created by Fabian Vogelsteller and Vitalik Buterin in November of 2015. But ERC 20 simply wasn't designed for security tokens and left a number of gaps. Numerous entities tried to address the shortcomings with proprietary implementations, including the DS protocol from Securitize, R-Token from Harbor, T-Rex from Tokeny and ST20 from Polymath. This multitude of approaches quickly created friction for the rest of the industry. Chiefly, custodians, exchanges, and other participants needed to perform extensive due diligence on the code associated with the tokens themselves, in addition to the standard business due diligence.

To tackle this problem, Polymath brought together 25 companies including custodians, lawyers, exchanges, auditors, KYC providers, former regulators, and transfer agents to propose a unified standard for security tokens on Ethereum. The goal was to ensure that the token's code met specific requirements in order to allow organizations to integrate it without costly and time-consuming technical due diligence. This standard, ERC 1400, has since been broadly embraced by the industry and adopted by organizations including ConsenSys and BNP Paribas.

ERC 1400 acts as an umbrella of standards and addresses requirements specific to the management of securities, including the ability to conserve UBO rights for custodied assets. Recognizing that regulation and the broader landscape continue to evolve, ERC 1400 was designed to be modular so new functionality could be added as required.

From ERC 1400 to Polymesh

ERC 1400 goes a long way towards making Ethereum more suitable for securities, but as a general-purpose chain, there are still gaps in functionality and scalability.

Because ERC 1400 has been so widely adopted, Polymath has been able to gather market feedback and use it as a foundation to build the first blockchain specifically for security tokens. Once the Polymesh Blockchain Initiative goes live, it will further enhance standardization and expedite tokenization efficiency. Issuers who used Token Studio on Ethereum will have the option to migrate their token over to the new chain.

CHALLENGE #2

Purpose misalignment

In addition to eliminating technical due diligence, ERC 1400 resolves some of the challenges surrounding security token management by automating transfer control, including the need for KYC verification, and corporate actions, like capital distribution or voting. Despite these advances, standards can only take us so far. Because of the breadth of use cases managed by Ethereum, the chain falls short when it comes to the intricacies of managing securities.

Firstly, on Ethereum, digital assets are programmed using smart contracts and as a result, custodians, exchanges and other market participants have to integrate each asset into their environment individually. But beyond that inefficiency, Ethereum's usage of probabilistic finality is a barrier to making it the golden record for asset ownership and the chain does not provide any affirmation mechanism, hence the airdrops we've all experienced.

As the industry has evolved, it's become clear that four keystone issues with asset tokenization on general-purpose blockchains that need to be addressed in order to align the functioning of the blockchain with the requirements of modern capital markets.

Identity

Securities issuance and transfer requires a known identity, but most chains are built for pseudonymity.

Governance

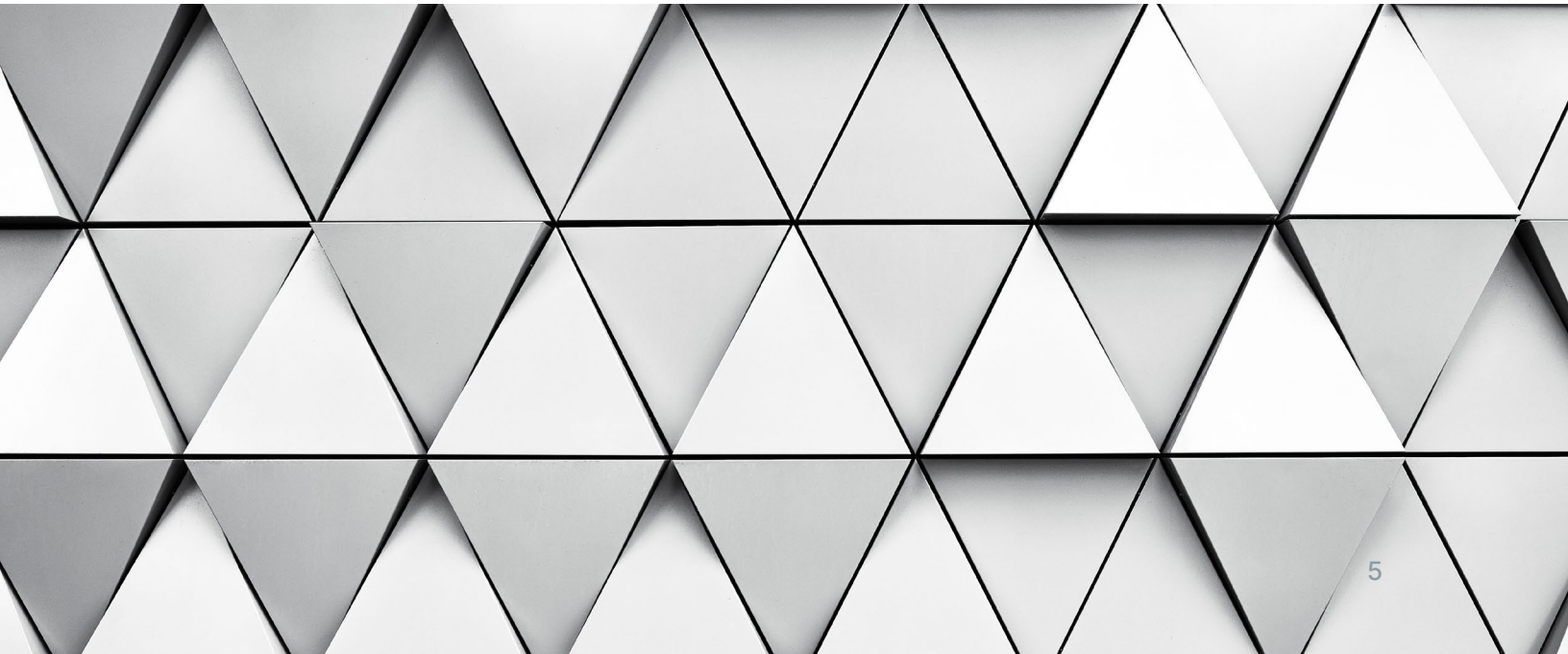
Contentious forks in the chain present significant legal and tax challenges for tokens that are backed by real assets.

Compliance

Security tokens are subject to a growing number of regulations, but chains struggle with complex logic needed to comply.

Confidentiality

Most market participants need their position and trades to remain confidential, but anyone can see holdings on general-purpose blockchains.



How to overcome the challenges

OPTION 1

Address through layer 2

Some of the functionality required for security token custody can be added though layer 2 solutions. Built on top of the chain, these layer 2 applications can automate key steps, but as users begin to layer on successive rules, the number and complexity of operations can push the chain to its computational limits. This drives up costs and processing time and makes it difficult to deploy complex logic at scale. Beyond that, layer 2 solutions can come at an unworkable compromise—to add transaction privacy, they must sacrifice the ability to configure compliance rules or enable key reporting capabilities, such as ownership.

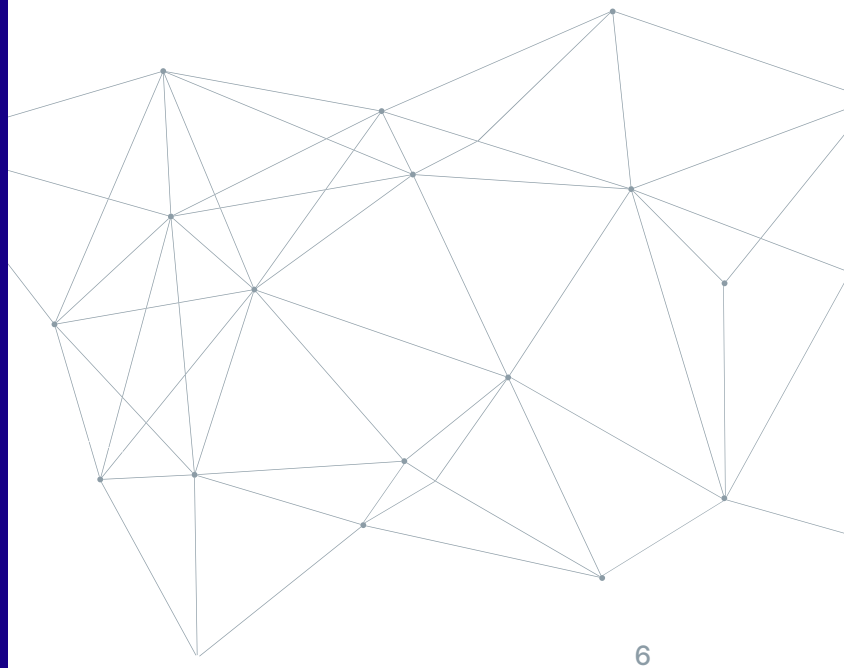
OPTION 2

Address with a purpose built blockchain

At a certain point, it makes sense to create a purpose-built infrastructure, rather than try to continue to build on top of one intended for other uses. While this requires a new ecosystem to come together, it bypasses the painful phase of small incremental improvements and provides major leaps forward in functionality. Polymesh is an institutional-grade permissioned blockchain built specifically for regulated assets. It streamlines antiquated processes and opens the door to new financial instruments by solving regulatory challenges with public infrastructure around identity, compliance, confidentiality, and governance through key design principles built into the base layer of the chain, rather than as external add-ons.

Requirements to support security tokens on blockchain

- **Deterministic finality**
- **Trade affirmation**
- **Fork resistance**
- **Built-in identity**
- **Scalable compliance**
- **Privacy and confidentiality**
- **Proof-of-stake consensus mechasnism to support ESG initiatives**



The advantages of a purpose-built blockchain for security token custody

A purpose-built blockchain can address issues with the public infrastructure and empower digital asset custodians to be more efficient and provide their clients with a more engaging experience at every stage.

STAGE 1

Identity Verification

Challenge with general purpose blockchains

Anonymity is a key principle of many blockchains, but this ethos makes it very difficult to meet compliance requirements around identity verification and to fulfill Know-Your-Customer (KYC) obligations. Today, most financial service providers comply with identification requirements by examining government-issued ID or other documents, which can be a slow and often manual process.

How a purpose-built chain can overcome it

Polymesh creates a single identity on the chain for each real-world individual or organization and then attaches attestations to it as needed. This modular two-stage approach to identity verification allows for efficient onboarding as well as specific checks. It also ensures that any accounts a user creates, or assets they hold or transfer, will be securely and confidentially connected to their identity.

Building identity into the core of the chain brings a few key advantages.

Sybil resistance

Each individual or entity can only have a single identity, which prevents an attacker from creating many pseudonymous digital identities to gain undue influence over the chain.

Simplified compliance

Unlike on public blockchains, tokenholders can't subvert rules by holding assets under multiple digital identities.

Known participants

Trades need to be determined by known, trusted, regulated entities. As a permissioned chain, transactions are validated by verified capital market participants that meet specific criteria.

Confidentiality

With confidential assets enabled by MERCAT, Polymesh makes it possible to maintain trade and position confidentiality without sacrificing compliance automation or auditing.

STAGE 2

Asset Onboarding

Challenge with general purpose blockchains

Most digital securities are programmed using smart contracts, which means that each new token needs to be individually integrated into the custody environment. Standards like ERC 1400 make this process much more efficient because they standardize the token configuration and eliminate the need for technical due diligence, but there is still room to make the process faster and more automated.

How a purpose-built chain can overcome it

Polymesh is built on the foundation established by ERC 1400, but in contrast to general purpose blockchains like Ethereum, assets on Polymesh are created at the protocol layer, which means that instead of creating a smart contract for each asset, the issuer calls a function and the protocol creates the token natively. As a result, custodians, exchanges, and other market participants can integrate once with the Polymesh blockchain and then quickly onboard new assets, rather than integrating each asset individually.

Assets on Polymesh are created at the protocol layer and as a result custodians and exchanges can integrate once and then onboard new assets quickly.

STAGE 3

Institutional-Grade Safekeeping

Challenge with general purpose blockchains

Regardless of the asset type, security is always top of mind when it comes to custody, but regulated assets present additional complexities, especially when issued or acquired by institutions rather than individuals. In fact, 76% of institutions considering digital asset custody services rank security as the most important factor. When security tokens first came to market, it wasn't possible to recover assets in the event of a loss of private key or to segregate duties. While we've come a long way, most chains are still broadly intended for use by individuals and don't offer the deeper enterprise safeguards that institutional users require.

How Polymesh overcomes it

Polymesh is purpose-built for institutional management of security tokens, and numerous mechanisms have been built into its core to help minimize external threats and maintain internal divisions of responsibility.

Portfolios

Built for enterprise, Polymesh lets issuers and investors organize assets into portfolios however they see fit and assign granular permissions. This structure allows large organizations to segregate duties and ensure each individual or organization can only access specific assets or perform specific actions, without compromising on compliance by using multiple accounts. Portfolios can also be used to efficiently grant custodial access to multiple assets.

Multi-signature

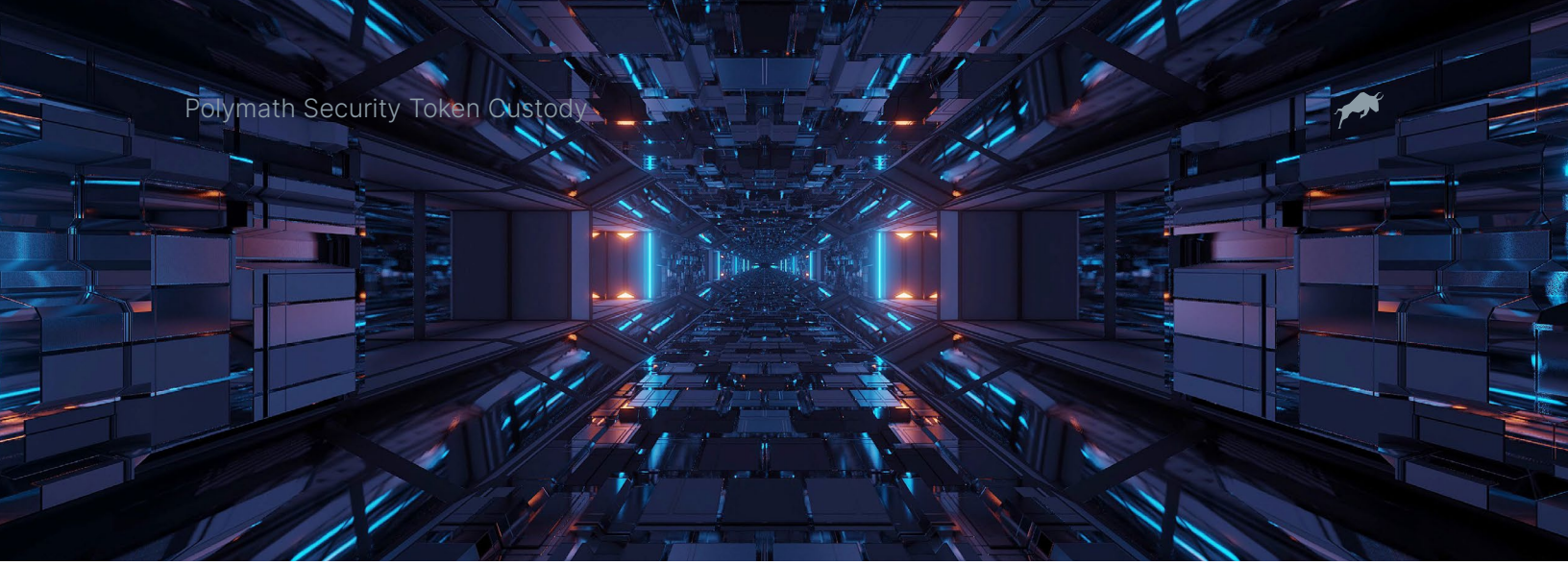
Usually, transactions are 'signed' by a single account. Multi-sig based accounts can be more secure because they require a combination of multiple keys to sign a transaction for it to be considered valid by the blockchain —acting as a failsafe against a single point of failure and spreading responsibility between multiple parties. When layered on top of a general-purpose chain through smart contracts, this functionality adds significant complexity, cost and processing time. Polymesh bypasses this issue by natively supporting multi-sig based accounts in its base layer.

76%

of institutions considering digital asset custody services rank security as the most important factor.

Layer 2 friendly

Polymesh offers an extensible and modular framework that brings best-of-breed security token management capabilities and offers open integration with other proprietary solutions. Polymesh can connect seamlessly with bespoke safekeeping solutions to protect assets under custody from multiple angles.



STAGE 4

Asset Servicing

Challenge with general purpose blockchains

In 2020, 87% of global asset managers, wealth managers, custodians, clearing houses and investment banks were still processing at least some of their corporate actions manually. This approach is labor intensive, error prone, and creates additional risk. Blockchain can bring significant automation to corporate actions, but according to the ISSA, adoption hinges on "strong governance and auditing principles to provide issuers, investors and regulators with assurance that they behave and deliver entitlements as issuers intend."

How a purpose-built chain can overcome it

Because Polymesh is purpose-built for security tokens, governance and auditability are core aspects of the chain's architecture. It is therefore able to automate the corporate actions lifecycle so that custodians can increase efficiency and decrease errors and overhead. The issuer inputs a few details to create a corporate action—from there, the engine will determine entitlements, schedule the communications*, distribute capital (if required), and update records. With all stakeholders working from the same instructions and looking at the same record, the process can move from one stage to the next without manual intervention, 'broken telephone' errors are significantly reduced, and issuers and investors get faster access to decision-critical position updates.

There are three main classes of corporate actions that can be automated:

Benefits

Events (predictable and non-predictable) that result in an increase to the position holder's securities or cash position, without altering the underlying security.

Re-organizations

Events that reshape or restructure the position holder's underlying securities position, possibly also combining a cash element.

Issuer Notices

Events used for the dissemination of information from the issuer to position holders, but that result in no change to

*Coming soon

STAGE 5

Transaction Settlement

Challenge with general purpose blockchains

Three years ago, Accenture conducted a study finding that blockchain technology stood to reduce settlement costs by 50% and in theory, 95% of trade processing and settlement can be automated through blockchain. As it stands today, there is still a large gap between what is possible and what is practical.

There are a number of challenges on general purpose blockchains, including:

Delivery failure
The DTCC ranks delivery failure as one of the main three reasons why settlements fail. On general-purpose blockchains, this is because users are able to agree to a transfer without delivering the assets, or agree to multiple transfers with the same set of assets.

Pre-funding
Participants in a blockchain transfer are required to part with cash or assets in advance by pre-funding their transaction to mitigate counterparty credit and liquidity risks.

Settlement finality
General purpose blockchains, like Ethereum, depend on probabilistic finality and never entirely finalize transactions.

Unwanted transfers
These transfers (often referred to as airdrops) present regulatory and operational concerns and have associated AML and taxation implications.

95%

of trade processing and settlement can be automated through blockchain.

> *Trade failures are surprisingly costly when all factors are taken into account. The stock may have been borrowed, incurring additional interest costs and the fail may have to be funded in cash. If it's near the month's end, it could impact the balance sheet with commensurate effects on regulatory requirements. On top of all this is the time spent by staff addressing the claims, penalties, cancel and correct fees and manual verification. Global Custodian reports that a global failure rate of just 2% is estimated to result in costs and losses up to $3 billion.*
>
> The Depository Trust & Clearing Corporation

Source.

How a purpose-built chain can overcome it

Polymesh provides a simplified approach to transfers that relies on efficient workflows and blockchain automation.

In so doing, it narrows the gap to blockchain settlement in three key ways:

Reduces delivery failures without pre-funding

The Polymesh Settlement Engine immediately commits assets once a settlement instruction is affirmed so that they cannot be spent in other transactions. Because this is done at the protocol layer, assets do not need to be sent away in advance of the transaction and asset transfer can happen on an atomic basis without requiring a smart contract to hold custody of both assets.

Provides deterministic transaction finality

Polymesh can provide the needed deterministic transaction finality through the GRANDPA finality gadget, an industry-led governance model, forkless upgrade process, and a comprehensive compliance validation framework.

Prevents airdrops and unwanted transfers

Polymesh's approach to asset transfers eliminates airdrops (tokens appearing in user wallets unprompted). Because users are required to affirm settlement instructions before tokens appear in wallets, custodians can be confident they aren't holding unaccounted for assets.

STAGE 6

Network Participation

Challenge with general purpose blockchains

With traditional proof-of-work blockchains, rewards for securing the chain and the ability to participate in the direction of the chain are out of reach for most participants. These chains are also susceptible to contentious forks, which can expose major legal and tax challenges for tokens backed by real assets.

How a purpose-built chain can overcome it

Polymesh's proof-of-stake consensus mechanism and on-chain governance process ensures that custodians and their clients are able to engage in decision making and share in rewards.

Governing Council

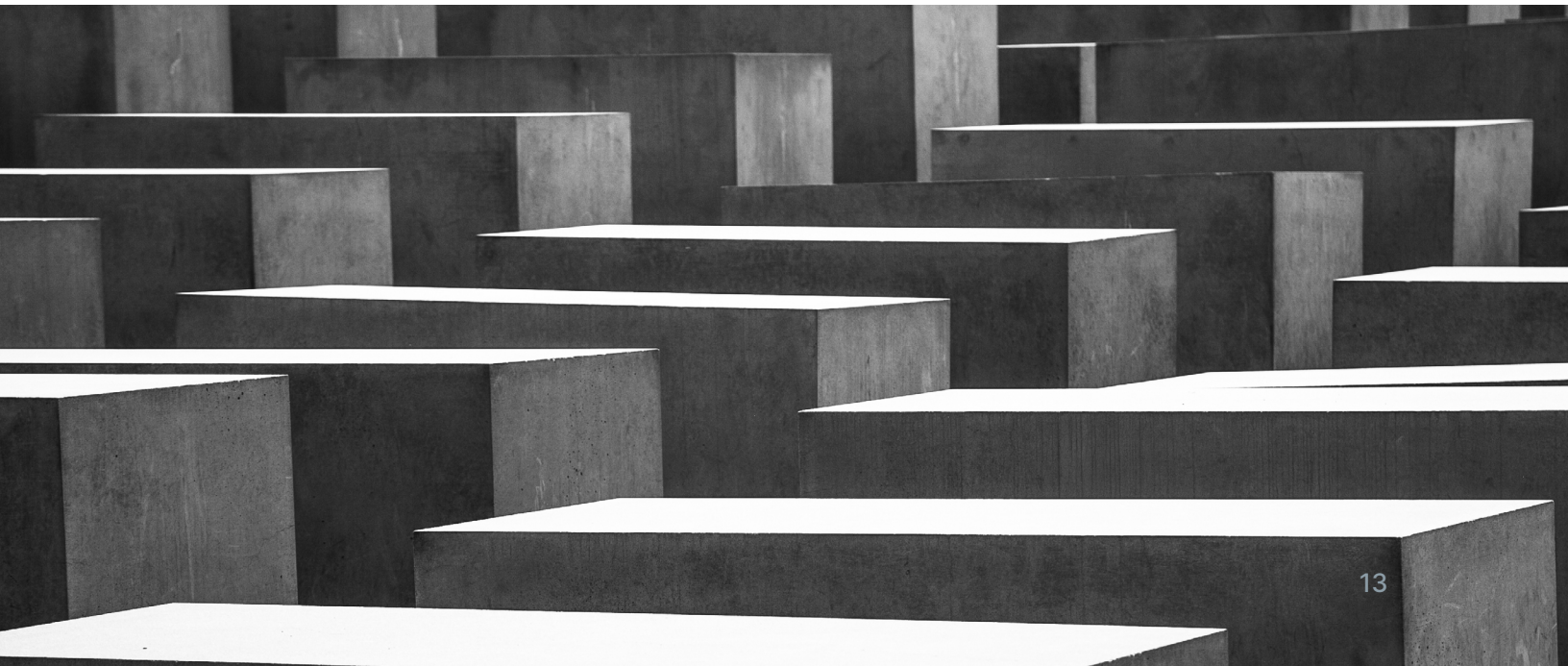
Polymesh relies on a council of key stakeholders to review Polymesh Improvement Proposals (PIP) submitted by committees or token holders, find consensus, and chart a path forward for its future development. The Governing Council, combined with Forkless Runtime Upgrades, lets Polymesh avoid forks and give custodians and other stakeholders a greater ability to participate in the evolution of the chain.

Node operation

Custodians (and other regulated entities) can earn rewards for the proper writing of blocks, and benefit from a purpose-built blockchain without creating one from scratch.

Staking

Institutions and their clients are becoming increasingly interested in staking and the rewards it can offer. Polymesh allows users to stake on operators, and both are rewarded or fined by the network based on blocks being added to the chain and fulfillment of their role.



Overcoming the constraints of legacy infrastructure

In many ways, the situation we are facing right now is not that different from one we faced 30 years ago with the internet. Home internet was initially run using existing phone lines. Intended just to carry voice, speed was severely capped and content delivery had to follow very strict rules.

In 1991, phone lines could handle 14.4 kilobytes per second. 7 years and millions of dollars of R&D later, speed had increased by four times—and the connection was still painfully slow. The industry was constrained by legacy infrastructure that prevented new services from being delivered, or even imagined.

Much like the early internet, attempting to use a pervasive but not fit-for-purpose infrastructure provides slow incremental benefits to securities operations, but leaves the true transformative potential on the table.

To manage security tokens on a general-purpose blockchain, there is a need for:

- **Identity on top of a chain that was built for pseudonymity**
- **Compliance on top of a chain that was built for censorship resistance**
- **Confidentiality and privacy on top of a chain built for transparency**
- **Deterministic finality on top of a chain that relies on probabilistic settlement finality**

Instead of going through that painful phase of small incremental improvements, transitioning to purpose-built blockchain for regulated assets enables innovation and gives custodians and other market participants the right tools to get in front of the growing security token market.

> *We stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another. In its scale, scope, and complexity, the transformation will be unlike anything humankind has experienced before.*

Klaus Schwab, Founder and Executive Chairman, World Economic Forum

Source.

POLYMATH

polymath.network

About Polymath

Polymath makes it easy to create, issue, and manage security tokens on the blockchain. Over 200 tokens have been deployed using our Ethereum-based solution and we are now in the midst of launching Polymesh, an institutional-grade blockchain built specifically for regulated assets. It streamlines antiquated processes and opens the door to new financial instruments by solving the inherent challenges with public infrastructure around identity, compliance, confidentiality, and governance.

Learn more