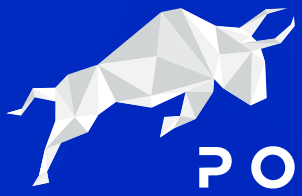


POLYMATH

Polymesh

Whitepaper

Adam Dossa
Graeme Moore
Jesse Lancaster
Michael Buchanan
Pablo Ruiz

January 29, 2020

Executive Summary

Security tokens have the ability to alter the financial landscape, unlocking trillions of dollars in asset value and investment, programmably automating operations, and driving new paths to liquidity. For Polymath, the Ethereum blockchain has been an excellent starting point for security tokens, but is missing foundational elements that issuers and investors need, and that institutions and regulators require. After having enabled the creation of 150+ tokens, our research and experience has shown that institutions need a blockchain built from the ground up with the specific requirements of securities regulations in mind.

Polymath addresses this need with Polymesh, an enterprise-grade blockchain built for security tokens. The foundations of Polymesh are focused on the most crucial regulatory elements, addressed by four key design principles meant to meet the demands of regulators and institutions, while unlocking the true potential of security tokens:

1. **Confidentiality** - protecting information and ownership privacy while providing a mechanism for accurate reporting and auditing.
2. **Identity** - ensuring that no individual or entity can create, acquire, or sell security tokens without a validated identity. Securities regulation requires issuers, in certain instances (i.e. issuances under exemptions), to know the identity or confirm the profile of their investors prior to investment, and continuously monitor their suitability throughout their investment. Additionally, all Validators must be known, regulated entities.
3. **Governance** - providing an operating and governance structure for how Polymesh is managed that allows for curation, and protects assets from contentious forks during network upgrades. This includes providing an established method for addressing and actioning proposals.
4. **Compliance** - providing financial primitives and smart extensions to manage security tokens across one or more jurisdictions and enforce appropriate rules for creating, issuing, and trading security tokens while also providing the capacity to manage necessary complex restrictions and distributions on-chain.

Polymesh will use the Nominated Proof-of-Stake consensus mechanism with the finality gadget GRANDPA, and be supported by POLYX, the native protocol token. With Polymesh, Validators stake POLYX on the network and run authoring nodes, Nominators stake POLYX on Validators, and both are rewarded or fined by the network based on blocks being added to the chain and fulfillment of their roles. All POLY tokens currently existing on Ethereum will be able to be upgraded to POLYX at a 1:1 ratio.

Structured in this way, we believe Polymesh will fill the gap between security token technology and the needs of issuers, investors, institutions, and regulators.

Disclaimer

This document is for informational purposes only and does not create any obligations whatsoever on Polymath. This document is a summary of certain Polymath product development plans and the information contained herein is selective and forward-looking subject to update, expansion, revision, or amendment. Due to various risks and uncertainties, including but not limited to, technological developments and industry conditions, the actual performance and development of items described herein may differ materially from those reflected or contemplated herein. Polymath does not accept any obligation to provide recipients with any additional information, or to update, expand, revise or amend the information herein, or to correct any inaccuracies which may become apparent. Although all information and views expressed herein were obtained from good faith estimates and assumptions made by Polymath management, no representation or warranty, express or implied, is made as to the accuracy or completeness of the information herein, and no assurance is provided that actual results will be consistent with the descriptions and projections herein.

This document does not constitute an offer to sell, or a solicitation of an offer to buy, POLY or POLYX, nor does it amount to a commitment by Polymath to make such an offer or solicitation at present or an indication of Polymath's willingness to make such an offer or solicitation in the future. This document is not a prospectus and does not constitute or form any part of any offer or invitation to subscribe for, underwrite or purchase POLY or POLYX, nor shall it or any part of it form the basis of, or be relied upon, in any way, in connection with any decision relating to POLY or POLYX. This document is not, and should not be construed as, legal or financial advice. Recipients should conduct their own investigation and analysis of the information contained herein and are advised to seek professional advice relating to the legal, financial, taxation, technological, and other implications of matters herein.

Polymath disclaims any and all liability relating to any information contained in this document.

Table of Contents

1.0 Introduction

Security tokens are financial securities created using blockchain technology. Like traditional securities, they represent ownership interests in assets (equity, debt, real estate, etc.), but being created digitally (tokenized) allows them to unlock the power of the blockchain with enhanced features. Security tokens introduce benefits to the market like efficiency through automated operations, increased global liquidity pools, and the creation of new and unique financial assets.

The Ethereum blockchain has been the most widely used blockchain to create, issue, and manage security tokens. Ethereum creates unstoppable applications through smart contracts that efficiently manage regulatory rules embedded in an issuer's security token to unlock non-traditional assets and improve liquidity. For Polymath, the choice to utilize and launch our initial platform on Ethereum was an obvious one—a credible and secure foundational infrastructure gave us the opportunity to validate the viability of the security token market.

However, our experience on a general-purpose blockchain has helped us understand that Ethereum lacks key elements which, if not included, would hamper industry and institutional acceptance of security tokens. For instance:

- Identity is an after-thought, running counter to the core principles of Ethereum: pseudonymity and decentralization. This creates legal and compliance challenges for issuers and investors, such as entities in sanctioned countries running nodes to write to the blockchain.
- Confidentiality is not preserved, with positions, trades, and amounts being publicly visible.
- Governance presents significant risk and complexity to issuers due to hard forks during upgrades.
- Compliance is challenged when necessary security token functionality is hindered by transaction limitations.

With a dedicated, domain-specific blockchain built specifically with security tokens in mind, these elements can be included from the ground up. This will improve usability and optimize the consensus mechanism, driving adoption and recognition for the security token industry.

2.0 Architecture

2.1 Financial Primitives

General-purpose blockchains typically have few primitives, that is, features built at the core of the blockchain. Instead, elements including security tokens and their associated ownership, transfer, and other restrictions, are implemented as smart contracts on top of the blockchain resulting in scalability and performance challenges. However with Polymesh, financial primitives are built into the foundation of the chain. Polymesh financial primitives allow users to operate the blockchain with low predetermined costs while allowing third-party developers to deploy innovative decentralized applications (dApps) on top of the chain.

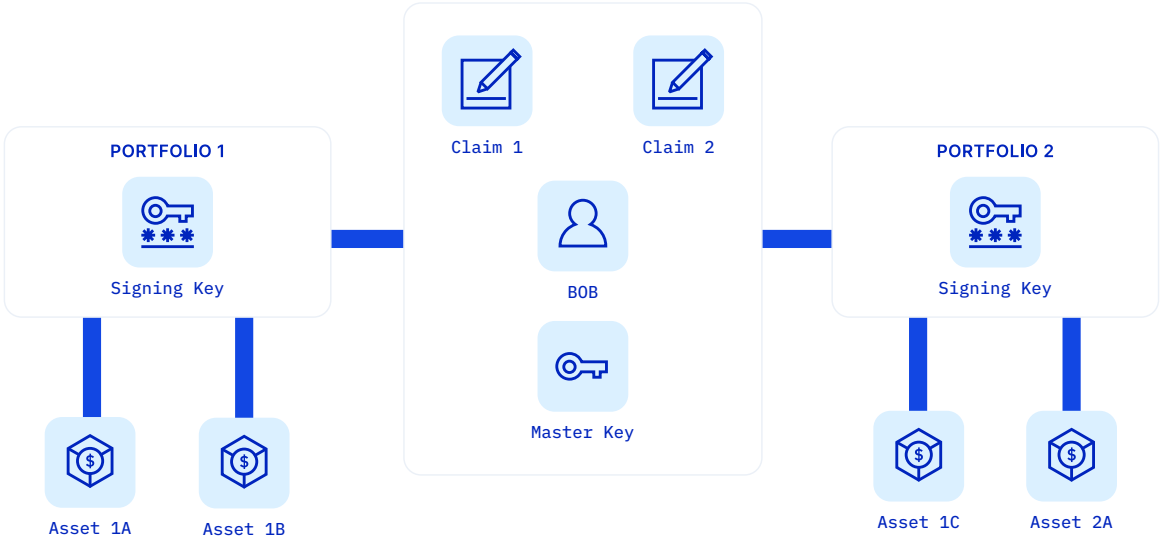
2.1.1 Regulated Assets

Regulated assets are the cornerstone of Polymesh. We use our industry-leading expertise that drove Polymath's leadership in the creation of the ERC1400 standard to help balance the challenges of open, transparent, and accessible global systems with jurisdictional compliance.

2.1.2 Identity

Identity is critical to every action with regulated securities. In order to present a flexible, global system of identity, we've made it core to the functioning of Polymesh; all actions on the chain are mediated through an identity, rather than through a simple public key like most public blockchains.

Identities are both universal (i.e. can be accessed throughout Polymesh) and permissioned—they collect a set of claims or attestations issued by network-approved or issuer-specific authorities about the owner of the identity. These claims can then be used to manage asset ownership, transfer, and other restrictions, as well as the operation of the blockchain's underlying consensus mechanism.



A single identity can have multiple asset portfolios allowing users to split assets for reporting and control purposes, while complying at an identity level.

Each identity has a single administration key, which can be used to add or remove signing keys from the identity. Signing keys can be used to execute actions through the identity, and also to deliver granular roles and permissions for identities and associated functionality within Polymesh.

As a member of the *Decentralized Identity Foundation*, as well as a participant in various standardization bodies, our approach to identity reflects these collaborations.

2.1.3 Record Keeping

The Polymesh blockchain captures all primary and secondary transfers of security tokens, allowing ownership data about those security tokens to be trustlessly captured on-chain while reducing information asymmetry between the issuer and tokenholders. Polymesh records exchanges of issued security tokens in a number of forms, from atomic settlement on-chain, to payment receipts from off-chain, third-party service providers.

2.1.4 Capital Distribution

Many assets have a cash flow associated with them. Polymesh allows issuers to distribute such cash flows by capturing ownership distribution data at fixed points in time. Issuers can determine the recipients of the distribution based on their identity or other criteria. They can use Smart Extensions *(see Section 2.3)* to perform complex calculations, determine the amounts to be distributed, distribute on-chain using digital assets such as stablecoins *(see Section 2.1.6)*, distribute off-chain using payment receipts, or distribute through a combination of on-chain and off-chain transactions.

2.1.5 Corporate Governance

Corporate Governance on Polymesh allows issuers to leverage the power of the public blockchain to combine transparency with techniques that allow tokenholders to vote on an issuer's corporate actions with privacy, while mitigating incentives to manipulate voting.

2.1.6 Stablecoins

In addition to security tokens, Polymesh supports stablecoins to facilitate activity on-chain such as cash distributions at a fraction of traditional costs. Stablecoins on Polymesh can be pegged to any currency and issued by adequately licensed and capitalized third-parties.

2.2 Economics

Polymath extensively researched and consulted with leading economic, game theory, and operational process experts to establish the token economy for Polymesh with the goal of delivering utility, security, and sustainability for the chain. The core of this economy is the native protocol token that fuels Polymesh, POLYX, which both secures and operates the blockchain. Any transaction or use of smart contracts on Polymesh is paid for in POLYX.

2.2.1 Enabling Economy

The consensus mechanism on Polymesh is Nominated Proof-of-Stake. Validators and Nominators work together to power Polymesh's enabling economy by staking within the network and acting according to the consensus rules. Participants receive rewards for successful validation of blocks to Polymesh. Validators and Nominators are not responsible for ensuring the compliance of a transaction, only that the transaction has been properly completed in accordance with protocol rules.[1]

Validators run authoring nodes that keep the blockchain secure and operational at all times. On Polymesh, Validators are permissioned entities, regulated in their respective jurisdictions. They earn block rewards as blocks are produced and finalized and may be penalized in the form of fines (slashing) for malicious, dormant, or incorrect activity. Prospective Validators may submit their application to the Economic Council for review and approval. *(See more on Governance in Section 5.0).*

Nominators select and stake Validators as a signal of trust. Their stake is distributed across their selected Validators using an algorithm that aims to evenly distribute all staked POLYX.[2] Any verified POLYX holder can become a Nominator. If the nominated Validators perform to protocol rules, the Validator and Nominator receive block rewards. Similarly, Nominators may be slashed based on a nominated Validator's improper activity.

VALIDATORS

Permissioned, regulated entities that process transactions and update Polymesh state

- Diverse regulated participants with known identity
- Incentivized through block rewards
- Responsible for running authoring nodes which must be available
- Directly participate in governance decisions and network upgrades

NOMINATORS

Unlimited number of POLYX holders who increase the security of Polymesh by staking their POLYX on their choice of Validators

- Validated identities (individuals or organizations)
- Share block rewards with their chosen Validators
- Receive feedback about Validators to inform their nomination decisions
- Participate in broader blockchain governance decisons

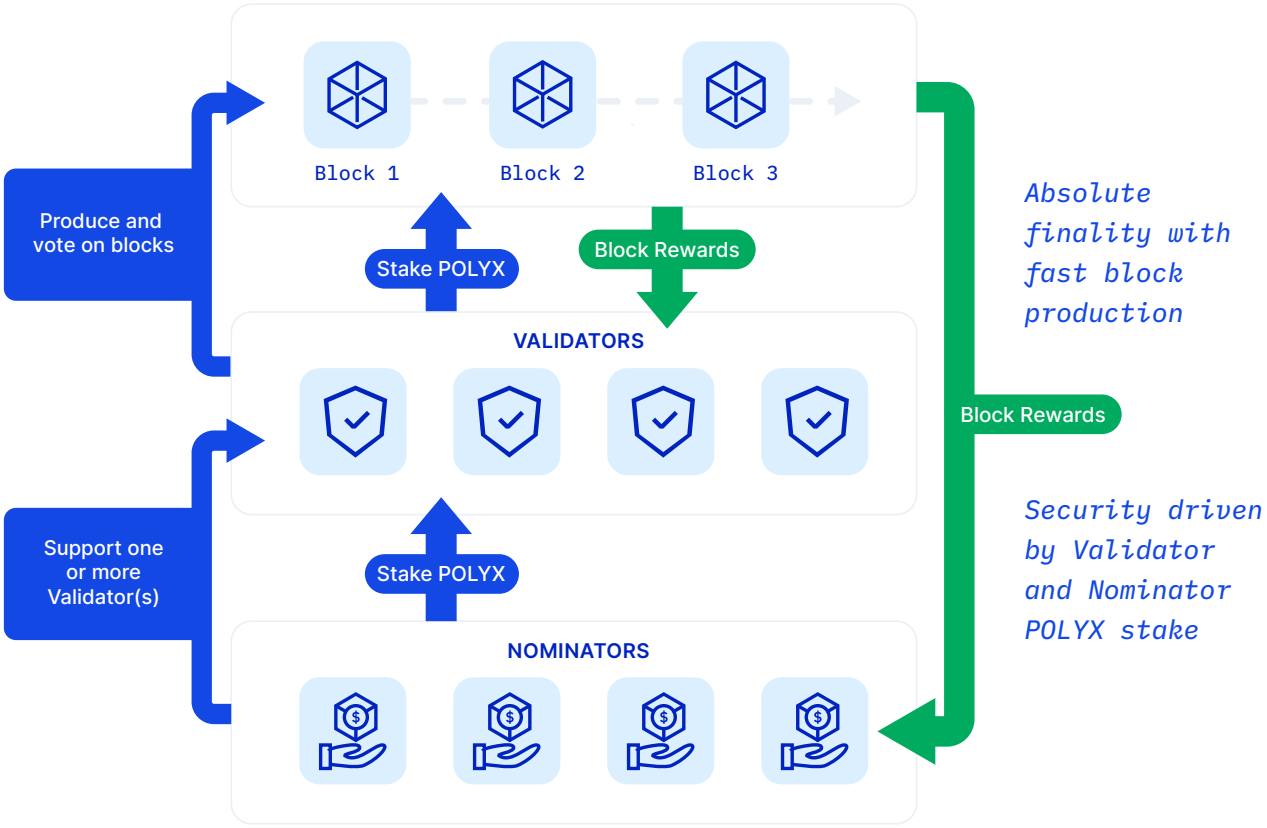
1. Web3 Foundation, "Intro to Nominated Proof-of-Stake," Research at W3F. https://research.web3.foundation/en/latest/polkadot/NPoS/index.html
2. Web3 Foundation, 2019, "Sequential Phragmen Method," October 30. https://wiki.polkadot.network/docs/en/learn-phragmen

Block Rewards are shared equally by all Validators that abide by the protocol rules. Validators keep a fixed percentage of the rewards with the rest being distributed to their Nominators on a pro-rata basis per their stake in the Validator.

Bonding Period is the amount of time POLYX is locked following a Validator or Nominator withdrawal request. Once requested, staked POLYX will unlock after the bonding period lapses. The bonding period may change through the governance process.

Finality

Nominated Proof-of-Stake offers deterministic finality that can be instantly trusted. Validators vote on the blocks generated, and once more than two-thirds of Validators have voted in favor of a block, it is finalized. A shared characteristic of blockchains is that every new block contains details of all the previous blocks and if a block is finalized, all its previous blocks are finalized as well. This characteristic allows finalizing a batch of blocks in one vote rather than having to vote on every block. Batching allows the chain to remain live and scalable with guaranteed finality within seconds rather than minutes.[3]



3. Alistair Stewart, 2019, "Extended Abstract: GRANDPA Finality Gadget," Research at W3F, Web3 Foundation, November 20, https://research.web3.foundation/en/latest/polkadot/GRANDPA.html#

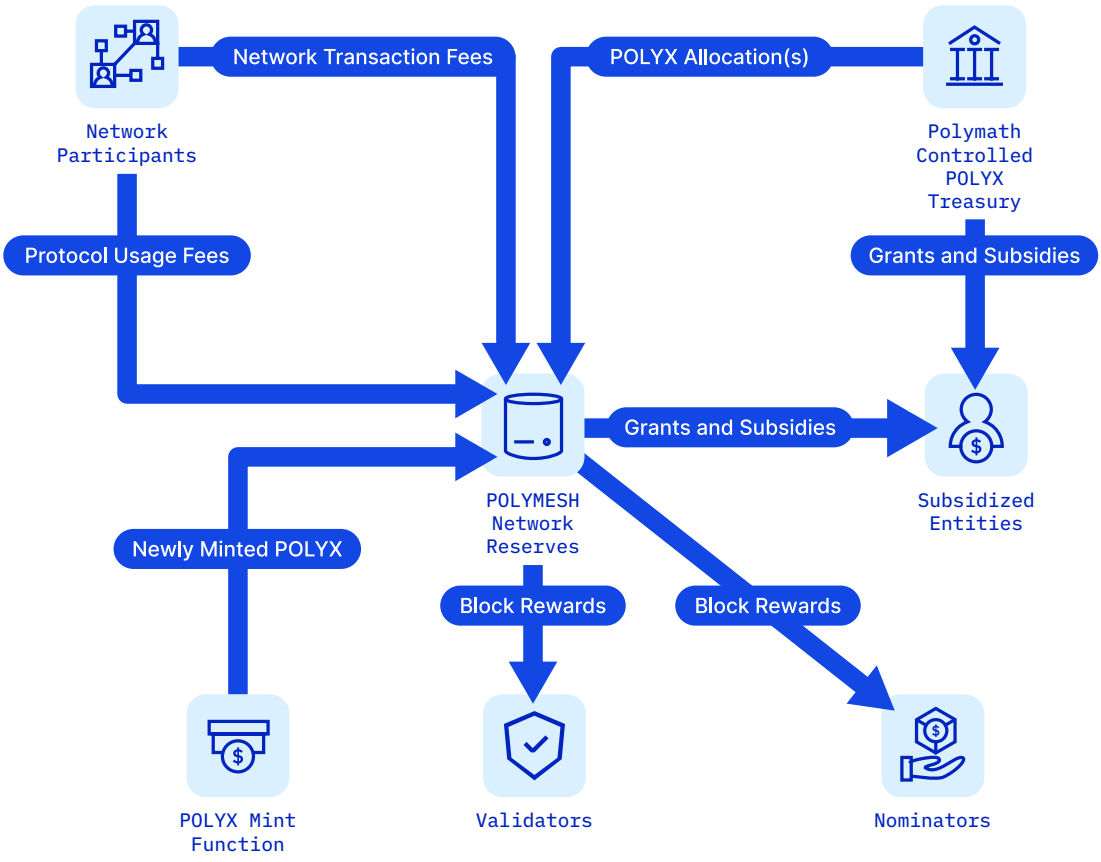
2.2.2 Internal Economy

The internal economy of Polymesh is driven by the objective to provide absolute finality, incentivize correct production of blocks, and build a sustainable and secure network.

Polymesh's Network Reserve is funded from three sources: direct transfers from Polymath's reserve currently held on Ethereum which unlocks over time; protocol usage fees (e.g. configuration of security tokens); and network transaction fees. POLYX is distributed from the Network Reserve based on the governance process that will likely evolve as Polymesh matures. Requests to disburse funds from the Network Reserve will be managed initially by Polymath, eventually being governed by POLYX tokenholder votes and the governing council. Funds will be used for purposes such as grants and subsidies to developers (including to Polymath developers over time), block rewards, or nominating Validators with POLYX.

Polymath's ERC20 protocol token, POLY, has a total supply of 1 billion tokens. We assume the majority of POLY will be converted to POLYX. The overall supply of POLYX over time will not be fixed, nor will it be subject to a predetermined upper limit. The supply of POLYX will increase in order to fund block rewards. The block reward mechanism will be designed so a sufficient proportion of POLYX at any point in time will be bonded to support the Proof-of-Stake consensus mechanism that underpins Polymesh. Block rewards will also be funded through network fees in addition to minting new POLYX. To stabalize the supply of POLYX during the initial stage of the Network's operation, Polymath will fund a pre-defined portion of the block rewards using POLYX migrated from Polymath's reserve on Ethereum.

Polymesh Network Reserve Overview



2.2.3 Enabled Economy

The POLYX fees at the core of Polymesh are required both to protect against denial-of-service (DoS) or spam attacks, as well as reward developers or organizations who build on Polymesh with additional customized functionality (e.g. providing compliance rules for specific asset classes and jurisdictions).

Polymesh has three classes of POLYX fees, all paid by the originator of the transaction:

- **Transaction fees** - these are the basic DoS protection mechanism. Broadly they are a function of the size (in bytes) and complexity (in storage / compute) of a transaction, but are otherwise agnostic to the type of functionality being used in the transaction.

- **Module fees** - these are fees for specific actions on the network such as issuing a new security token or dividend. They are set by Polymath and modified over time through a governance process.

- **Smart extension fees** - these are fees for third-party smart extensions found in the smart extension marketplace and set by those third-party developers (e.g. compliance rules). A predetermined portion of smart extension fees will be paid to the Network Reserve.

2.2.4 Token

POLYX is for use on the Polymesh chain, supporting the platform and serving the system in ways that include but are not limited to:

1. Fueling the enabling economy. Similar to ETH on Ethereum, POLYX will serve as gas on Polymesh. Transactions are paid for in POLYX (e.g. submitting transactions, running a smart contract) into the Network Reserve. This also funds system operational expenses.
2. Increasing system value creation. Funds from the Network Reserve will be paid as block rewards to Validators and Nominators for providing their computing resources, staking POLYX, and meeting standards of proper behavior. POLYX enables tokenholders to actively participate in the security of the blockchain by staking their POLYX to nominate Validators and earning a commission from block rewards.
3. Preventing spam. Attaching a cost in POLYX to transactions on the chain helps prevent network spamming.
4. Paying grants for projects that contribute to ecosystem growth and maintenance.
5. Managing upgrade governance. POLYX can be used to stake and vote for network upgrades.

POLY to POLYX upgrade mechanics

For at least one year from the launch of Polymesh mainnet, there will be a bridge to upgrade POLY to POLYX. POLY tokenholders can upgrade to POLYX tokens at a 1:1 rate. A significant amount of the Polymath POLY reserve will also be migrated through the same bridge. A validated identity is required to transact with POLYX tokens.

2.3 Smart Extensions

Smart extensions are the backbone of security tokens on Polymesh. Each smart extension will give issuers the ability to program specific rules into their security tokens, executing actions in a standardized way to satisfy an issuer's need for functionality and regulators' requirements for compliance. The Regulated Asset, Capital Distribution, Record Keeping, and Corporate Governance financial primitives can be adapted using smart extensions.

2.4 Third-Party Extensibility

Smart extensions can also be constrained in terms of their functionality to their specific domain. Polymesh allows third-party companies to develop extensions and deploy on-chain dApps which can leverage Polymesh's financial primitives to provide innovative open finance protocols and other related services.

3.0 Identity

All Polymesh users need to validate their identity with a verified service provider as part of their initial on-boarding. This gives each user a validated identity which is at the core of Polymesh. While this requirement adds friction to on-boarding, it provides a host of anticipated long-term benefits and utility to the blockchain, leading to potential rapid adoption by institutional and regulated users. Identity service providers will need to ensure the claims of Polymesh users remain up to date (continuous compliance). Additionally, some Polymesh issuers and tokenholders will need to be subject to other continuous checks, which may include Accreditation checks depending on the assets they invest in and their jurisdiction.

Particularly, validating identities in the initial on-boarding helps address a key challenge which most public blockchains ignore: sybil resistance. Sybil resistance blocks users from freely creating multiple on-chain identities. By adding this feature to the base layer of Polymesh, users can rely on the single identity and reputation of other users, a large barrier for more sophisticated open finance protocols.

Other benefits of identity at the base layer of the chain:

- POLYX provenance - this allows regulated entities, including institutions, to use and acquire POLYX tokens to access the network with the confidence that these tokens have a known provenance.

- Assurance - since all Validators and Nominators go through initial identity validation, the network will mitigate the risk of users making payments to or transacting with applicable restricted or sanctioned nations, entities, or persons.

- Validated identity for regulated assets - permits a tiered customer due diligence (CDD) approach that lets issuers use validated identity and enhance it with supplemental due diligence activities to meet their desired assurance level.

In order to facilitate every Polymesh user having a validated identity, there will be a set of identity service providers who are authorized to issue identity claims. This list of service providers will be maintained through the Polymesh governance process.

4.0 Confidentiality

Confidentiality is an integral element of regulated assets. Polymesh's confidentiality and privacy features are tailored to the needs of the financial industry and tackle three areas of concern:

1. Meeting ownership, transfer, and other restrictions without revealing confidential information;
2. Ownership privacy; and
3. Satisfying the first two points while ensuring the issuer is able to report and audit holdings of their asset.

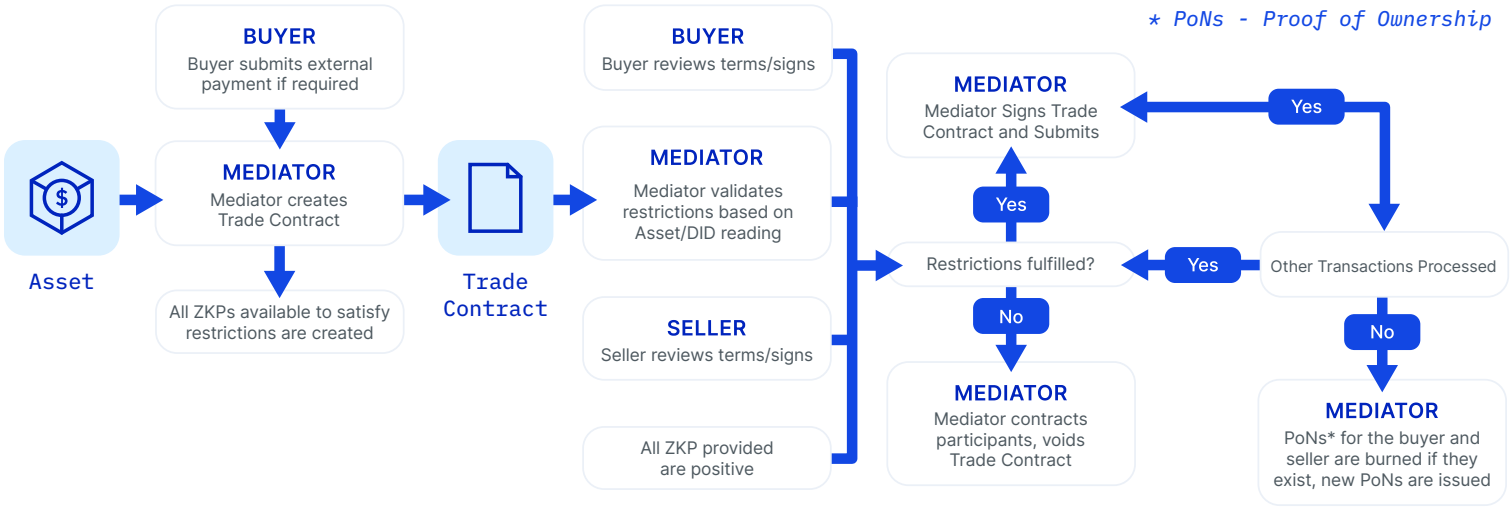
Confidentiality on Polymesh is met through a confidential transaction workflow.

4.1 Confidential Transaction Workflow

Our confidential transaction workflow allows us to safely mix cryptographic proofs with off-chain assertions. For example, when two parties wish to participate in an exchange on-chain, confidentiality works as follows:

1. The issuer (or trusted third-party / mediator) creates a trade contract on-chain.[4] This contract has a list of restrictions that need to be satisfied.
2. Zero knowledge proofs can satisfy some restrictions where available.
3. For other restrictions, a mediator can validate them off-chain and digitally sign that the restriction is satisfied.
4. Both parties digitally sign.
5. The transaction is completed on-chain.
6. Asymmetrically encrypted details are recorded back to the asset data storage where they can be used for reporting or to inform other transfer restrictions (e.g. percentage ownership restrictions).

See below diagram for visualization:



4. Trusted third parties / mediators are companies like exchanges, broker-dealers, etc. who handle anything from a single transaction to a raise, all on behalf of the issuer.

4.2 Auditability v. Privacy

One of the challenges for Polymesh when it comes to ownership privacy is that we use an account model instead of a UTXO model, making many of the existing schemes for preserving privacy during transfers not viable for Polymesh.[5] We resolve this challenge using a variety of cryptographic techniques. Further detail on these techniques will be discussed in a separate whitepaper devoted to privacy.

4.3 Issuer Reporting and Controls

As noted in 4.1, because of the trade contract and transaction workflow design, the details of transactions regarding the issuer's assets are always decryptable by the issuer regardless of the participants or mediator. On-chain it will be recorded as an encrypted blob, so any and all reporting and auditing can be done exclusively by the issuer.

4.4 Who Can See What

	Can See	Cannot See
Issuers[6]	• All transactions and details relating to their own assets	• Transaction data for other issuers' assets • Investor ownership of unrelated assets
Mediators	• Details for transactions they have mediated • Asset data required to verify trade restrictions	• Transaction data for transactions they did not mediate, unless an issuer has made this information available for satisfying transfer restrictions • Investor ownership of other assets
Investors	• Their own wallet balances • May be able to deduce when other parties are trading an asset they previously held, but not the quantity traded	• Transaction data relating to the asset outside their own transactions • Other investor ownership of other assets
Validators/ Nominators/ Public	• That a transaction has occurred between two parties	• Transaction amounts or assets

5. Rui Zhang, Rui Xue, Ling Liu, 2019, "Security and Privacy on Blockchain," Association for Computing Machinery, August 16, 7-9, https://arxiv.org/pdf/1903.07602.pdf
6. Regulators can request details from issuers directly.

5.0 Governance

Polymesh is governed by a main council, with a set of specialized sub-councils:

- Governing Council overseeing all councils with the ability to create or dissolve councils
  - Technical Council overseeing network upgrades
  - Economic Council overseeing network economy, including POLYX emissions policy and fees
  - Ecosystem Council overseeing subjects related to meeting and exceeding security token ecosystem partner needs and ecosystem growth

Councils will be comprised of Polymesh Network participants and will be responsible for fulfilling governing duties related to their specific council, e.g. reviewing proposals and voting on them. Any Polymesh Network participant with a Polymesh identity can make a proposal to any council. Proposals need to be staked in order to prevent the system from spamming council members. The Governing Council is operated by Polymath and will be decentralized over time.

5.1 Network Upgrades

Forks during upgrades present a severe problem for traditional public blockchains that can cause duplicated instances of blocks, and in our case, assets. Polymesh features forkless upgrades through an on-chain governance process. The WASM runtime of Polymesh is directly stored on the blockchain through the governance process, so when a node is notified of a new upgrade, it pulls the latest version from the blockchain. Since the WASM runtime is stored on the blockchain itself, all the nodes have guaranteed access to the same version. This process also reduces overhead required to coordinate a network upgrade.

Managing network upgrades through on-chain governance also gives all observers of the chain a clear decision on the official version of the chain (i.e. the version which follows the on-chain governance protocols). This removes any uncertainty for users of the chain or requirements to establish operational governance around managing forks.

6.0 Compliance

On Polymesh, automated compliance of assets is both transparent and real-time to help simplify regulatory reporting for assets, remove the need for complex systems to track and authorize asset transfers, reduce operational costs, and lower barriers to liquidity.

Managing asset distribution and token ownership on Polymesh means issuers have the ability to enforce compliance in real-time with smart extensions representing different compliance rules. These smart extensions are used to validate asset transfers and provide flexibility when managing compliance for a mixture of asset types, jurisdictions, and offering types in a standardized manner. Smart extensions are provisioned by Polymath or third-party developers and made available to all Polymesh issuers. Issuers are responsible for selecting, configuring, and implementing the appropriate suite of smart extensions for their token offering to satisfy specific regulatory, contractual, or other requirements.

An example of how smart extensions operate:

- An asset is created that can be held by a maximum of 1,000 investors, and no single investor can hold more than 10% of the asset.
- Two separate smart extensions would manage a rule each (maximum number of investors, and maximum percentage ownership), approving or denying transfers based on these rules.

Polymesh also standardizes management of asset compliance through the identity primitive. Issuers govern who can hold assets and under which conditions by creating rules based on investor identity claims. For example, issuers can restrict ownership of their asset to investors that have completed specific know-your-client and anti-money laundering (KYC/AML) processes or can manage transfer restrictions that apply to their employees or affiliates.

7.0 Standards and Interoperability

While Polymesh is a stand-alone blockchain, there are some cases where the advantages of bringing assets from other blockchains to Polymesh can be powerful.

7.1 ERC1400

On Ethereum, Polymath led the creation of The Security Token Standard (ERC1400) to address financial institutions' need for consistency in how assets are created and handled. ERC1400 is a library of standards to guide the efficient and effective creation of compliant security tokens. Specifically, it includes: ERC1594, the core security token standard; ERC1643, the document management standard; ERC1644, the controller token standard; ERC2258, the custodial ownership standard; and ERC1410, the partially fungible token standard. Polymesh models assets and compliance following the ERC1400 specification, providing a standard approach to assets and compliance across both our Ethereum protocol and Polymesh.

7.2 Relay Chains

One route to interoperability is via a relay chain. Relay chains like Polkadot aim to provide a decentralized interoperability layer allowing different networks to atomically communicate and exchange state. They have different trade-offs around security, user experience, and the necessary Validators that can monitor the relay chain and its interacting blockchains. There are no immediate plans to have Polymesh run on a relay network. However, the architecture is designed to leave the option for consideration in the future.

7.3 Wrapped Assets

Polymesh seamlessly supports various types of wrapped tokens, along with other open finance protocols. For these assets that originate on other blockchains, it is possible to have a bridge or series of bridges that can move them to Polymesh. Assets will be locked on their original network, then re-minted as a wrapped token on Polymesh. They can subsequently be bridged back by destroying them on Polymesh and unlocking them on their original network.

7.4 Migrated Security Tokens

Polymesh provides a streamlined process to allow issuers of existing regulated assets to migrate those assets over to Polymesh to take advantage of unique features and optimizations. This process may be complex for pre-existing assets with many investors as these investors need to be individually migrated. To mitigate this concern, Polymesh provides placeholder identities and accounts that can be used for existing investors who have not yet migrated to the chain. These placeholders can be trustlessly claimed by those investors on Polymesh when they wish to interact with the asset they own.

8.0 Oracles and Market Data

Polymesh leverages industry standards to define how to reference or retrieve various types of market data. It relies on a federated security model through Validators or market data providers acting as trusted oracles.

8.1 Validator Market Data (Off-chain Workers)

Polymesh integrates major market data providers through a network of permissioned and reputable Validators, who fetch data for requestors on-chain. This uses a method called off-chain workers, encompassing tasks longer than a single block that Validators use to retrieve and provide data from external (non-blockchain) sources.

8.2 General Market Data (Signed Data)

Market data can also be requested from specific data providers using the same process as above. This data is then signed using known and established public keys of those providers and validated on-chain before the market data is accessed. This approach relies on trusting a single market data provider to share correct data and secure their private keys.

Further Reading

Governance

Institutionalization of Cryptoassets
https://assets.kpmg/content/dam/kpmg/us/pdf/2018/11/institutionalization-cryptoassets.pdf

Confidentiality

AZTEC Privacy Protocol
https://www.aztecprotocol.com/

Zether: Towards Privacy in a Smart Contract World
https://crypto.stanford.edu/~buenz/papers/zether.pdf

Anonymous Zether
https://github.com/jpmorganchase/anonymous-zether

ZkVM: Fast, Private, Flexible Blockchain Contracts
https://github.com/stellar/slingshot/blob/main/zkvm/docs/zkvm-design.md

Lelantus: Towards Confidentiality and Anonymity of Blockchain Transactions From Standard Assumptions
https://eprint.iacr.org/2019/373.pdf

Bibliography

Stewart, Alistair. 2019. “Extended Abstract: GRANDPA Finality Gadget.” Research at W3F. Web3 Foundation. November 20. https://research.web3.foundation/en/latest/polkadot/GRANDPA.html

Zhang, Rui, Rui Xue, and Ling Liu. 2019. “Security and Privacy on Blockchain.” Association for Computing Machinery. August 16. 7-9. https://arxiv.org/pdf/1903.07602.pdf

Web3 Foundation. “Intro to Nominated Proof-of-Stake.” Research at W3F. https://research.web3.foundation/en/latest/polkadot/NPoS/index.html

Web3 Foundation. 2019. “Sequential Phragmen Method.” Polkadot Wiki. October 30. https://wiki.polkadot.network/docs/en/learn-phragmen

Authors
Adam Dossa
Graeme Moore
Jesse Lancaster
Michael Buchanan
Pablo Ruiz

Acknowledgements
Brian Poleck
Chris Housser
Mohammed Muraj
Mudit Gupta
Thomas Borrel
William Vaz-Jones

And a special thanks to the institutions, industry stakeholders, and the Polymath community who provided their comments and feedback.