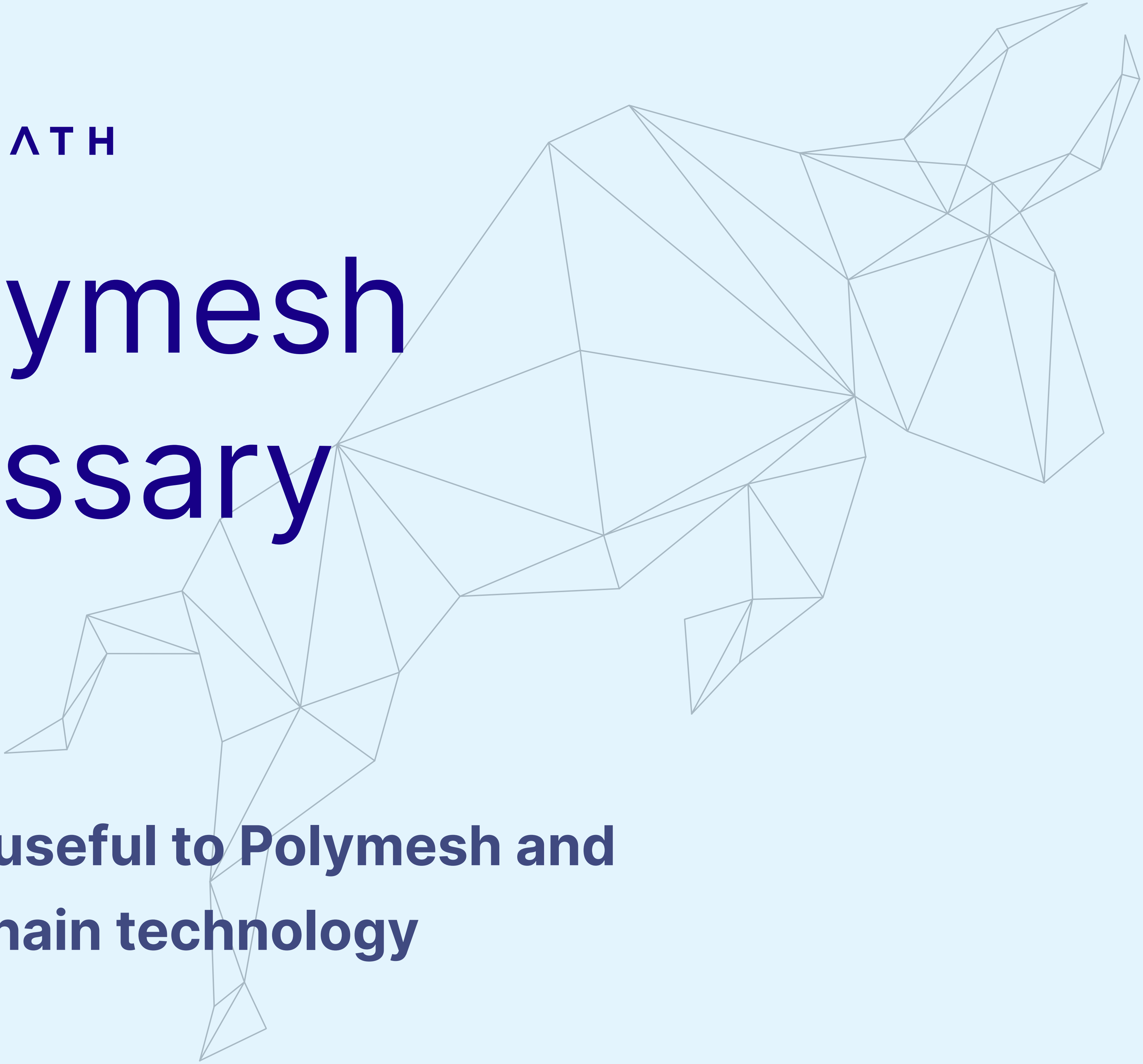
POLYMATH

Polymesh glossary



Terms useful to Polymesh and blockchain technology

Polymesh glossary

A glossary of terms useful to Polymesh and blockchain technology.

Just like how the Internet ushered in a new era, blockchain technology is opening up new opportunities and bringing possibilities for innovation that weren't previously conceivable.

As with the advent of any new technology, the era of blockchain is also bringing new vocabulary (what even is a blockchain?), as well as ushering in new ways of using pre-existing concepts (for example, digital assets).

To make it easy, we've created the Polymesh Glossary: a list of explanations for common terms you'll find when we talk about Polymesh– covering everything from distributed ledger technology (DLT) to nominated proof-of-stake (NPoS), Sybil attacks and forks.

While the vernacular is constantly evolving with advances in the space, these basic definitions will provide a good starting place to understand how Polymesh works and the nuances of its structure and operations.

Contents

DLT, blockchain, and the different types and layers

Tokenization: tokens, their types, and standards

The crypto-economic system: consensus, proof-of-stake, and who's involved

Decentralization, governance, and transaction finality

Distributed ledger technology (DLT)

DLT is a shared, synchronized database that is distributed digitally across a system of multiple participants. Typically, new information is added to the ledger only once consensus is reached, at which point it is time-stamped and given a unique cryptographic signature. When all participants share a single view of the record, it provides a verifiable and auditable history of the information stored, which is why DLT is useful for transactions. By providing a single source of truth, DLTs can eliminate the need for an intermediary or central authority to process, validate, or authenticate transactions. That said, DLTs are not inherently decentralized, nor do they necessarily employ blockchains.

Blockchain

A form of DLT, blockchain underlies a distributed ledger and permits it to be shared collectively and securely, facilitating easier transaction recording and asset tracking. It differs from other forms of DLT in that it stores information in blocks that are chained together. New data comes in and is added to a new block, which is then chained onto the previous block, linking the chain in chronological order and preventing the erasure of previous blocks. Ultimately, blockchain can provide immediate, shared, and completely transparent information stored on an immutable ledger accessible by all network members. Its most common use is as a ledger for transactions.

General-purpose blockchain

A blockchain designed for multiple use-cases. Taking a lowest common denominator approach, these chains typically have few primitives or features built into their core. Instead, elements like security tokens and their associated ownership, transfer, and other restrictions are implemented as smart contracts on top of the blockchain. However, this ultimately results in scalability and performance challenges.

Purpose-built blockchain

A blockchain built with one use-case in mind– like Polymesh, which was engineered specifically for security tokens. With Polymesh, financial primitives are built into the foundation of the chain, allowing users to operate the chain with low predetermined costs while allowing third-party developers to deploy innovative decentralized applications (dApps) on top of the chain.

Testnet

A prototype blockchain environment where developers can test code, create or modify functionalities, and explore possibilities of new features without causing damage to the main blockchain. Tokens on a testnet are not tied to ‘real’ money and can be obtained at no cost for the purpose of testing transactions. Even once a mainnet has launched, testnets remain useful for developers working to build on or improve the network.

Mainnet

A project’s main blockchain network. Unlike the testnet, the Mainnet makes the chain available for use in a way that supports the project’s functionality and delivers value to users by tying tokens to real value, enabling users to make live ‘real-world’ transactions.

Protocol

The set of crypto-economic rules that govern how the blockchain operates, such as how and which kind of data is distributed and how consensus is maintained across the network. Most blockchains have one protocol each, and one native token per protocol. Using the native token, protocols create financial incentives that drive the network of participants and coordinate their behaviour for the continued operation of the chain.

Protocol layer

The first layer of the blockchain, sometimes aptly named ‘layer-1’ or implementation layer, this layer implements the protocol. It refers to the core architecture of the blockchain and is responsible for the entire network’s rules and parameters, including its consensus mechanism, computing language, block time, and anything else which ensures base-level functionality. On Polymesh, security and compliance are baked-in to the protocol layer, which defines how operations like staking and governance will work.

Layer-2

Second-layer solutions or layer-2 protocols are "off-chain" blockchain protocols that sit on top of the first layer to facilitate better operations. Layer-2 solutions improve scalability and interoperability and solve operational difficulties by handling interactions on behalf of the base network. Think of layer-2 solutions as something which interact with the chain and perform necessary functions for its operation, but don't perform those functions on the chain itself. On Polymesh, customer due diligence (CDD) would classify as a layer-2 protocol since CDD providers integrate with one common interface to onboard users onto the network.

Application layer

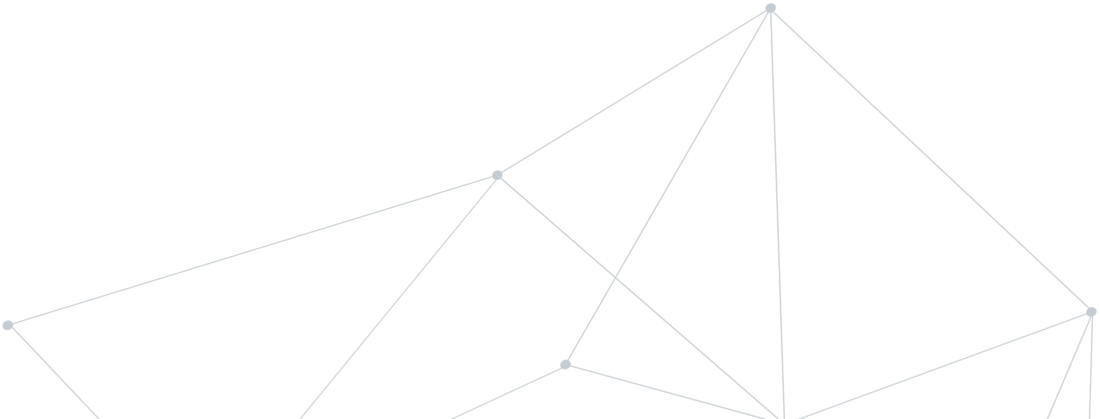
The third and outer-most layer of the blockchain consists of the user interfaces (UIs) that abstract or hide the technical details of the network's communication channel. This layer ultimately creates many of the real-world use cases for the blockchain. The main components are application programming interfaces (APIs), UIs, and scripts. There are many applications built on Polymesh including the Polymesh Dashboard, Polymesh Wallet, and Token Studio, as well as other service provider integrations or dApps.

Smart contracts

A set of logic rules in the form of coded script which can be embedded into the blockchain and executed automatically to govern processes like transactions. Smart contracts live on-chain as a and run exactly according to logic rules, enabling the code to mediate agreements and transactions without relying on a central authority. Programmable smart contracts make security tokens truly digital by managing asset attributes and automating functionality. Since smart contracts can create complexity in the end-to-end solution, assets on Polymesh are instead created at the protocol layer.

Decentralized applications (dApps)

Decentralized applications (dApps) are applications that run on top of a peer-to-peer network such as blockchain and operate in an open-source, public environment. Like other web applications, dApps enable real-world use cases of technology, but their back-end process differs in that it communicates on a decentralized network, i.e. a network with no centralized server. dApps rely on the blockchain to process and store data through the network and usually execute functions like transactions through smart contracts, which enables them to eschew control of an individual or company for the logic written into the contract's code.



Digital assets

Digital assets are broadly defined as digital representations of something of value. **In the context of blockchain, digital assets are created, traded, and stored on the blockchain, enabling ownership to be verified and recorded electronically.** This removes the need for paperwork or mediation by a central party like a bank or broker, making transactions quicker and easier. Cryptocurrencies, asset-backed stablecoins, security tokens and utility tokens are all subclasses of digital assets.

Tokenization

The digital representation of real-world assets on the chain, analogous to digital share certificates. Tokenization greatly improves upon inefficient and ineffective real-world functions tied to the creation, issuance, and ongoing management of securities. It brings benefits like increased efficiency, better transparency, and automated compliance, and has the potential to transform the market by improving liquidity and facilitating the innovation of new product offerings.

Security token

Like traditional securities, a security token is a financial instrument that represents ownership interest in an asset– only it’s been created digitally (tokenized) to unlock the power of the blockchain. **Put simply, security tokens are digital representations of financial securities on a blockchain.** Security tokens benefit markets by bringing greater efficiency through automation, increasing global liquidity pools, and facilitating the creation of new and unique financial assets. Because of their digital nature, security tokens may not only represent ownership of traditional assets like publicly traded equity or bonds, but also traditionally illiquid assets like private placements, real estate, or art. As with traditional securities, security tokens are subject to regulation.

Network protocol token

The token inherent to the blockchain's protocol. The network (or native) protocol token is distinct from the on-chain tokens, such as security tokens, that can be issued "on top" of the blockchain. On Polymesh, the network protocol token is POLYX. POLYX is used for paying transaction fees as well as a whole range of other functions related to the network's operations, such as participating in staking or voting on governance proposals.

Utility token

A token intended to provide access to a blockchain-based infrastructure, designed for use within that ecosystem only. Unlike security tokens, utility tokens are not designed as investments. Rather, holders of these tokens gain value in the form of utility or benefit. Utility tokens usually act as an access point into the network; without them, you can't access the platform or its corresponding products and services. Polymesh's network protocol token POLYX is a utility token based on guidance by the Swiss financial regulator FINMA.

Standards

Conventions guiding the development and use of blockchain technology. Security token standards like ERC-1400 go a long way towards making security tokens more viable on general-purpose chains by eliminating the need for technical due diligence and providing securities-specific features, but gaps in functionality and scalability on general-purpose blockchains remain.

ERC-1400

A unified standard for security tokens on Ethereum proposed by Polymath in collaboration with 25 other key industry players and adopted by many organizations since. Recognizing that regulation continues to evolve, ERC-1400 was designed to be modular so that new functionality could be added as required. Polymesh models assets and compliance inspired by the ERC-1400 specification, providing a standard approach to assets and compliance.

Consensus mechanism

A fault-tolerant mechanism that sets the roles, rules, and incentives for how consensus is achieved and information is written to the chain. Consensus on a single data value or network state is important for the chain's continuous functioning as a distributed process involving multiple nodes participating together across a decentralized computer network. Consensus mechanisms can refer to any number of methodologies used to achieve agreement, trust, and security across the network. The two most prevalent are proof-of-work (PoW) and proof-of-stake (PoS).

Proof-of-work (PoW)

Proof-of-work blockchains keep nodes in the network honest by requiring them to compete to create new blocks, rewarding them for most computational effort. The winner is typically whoever first completes a mathematical puzzle. Upon completion, the answer is verified and posted publicly to the chain, linking the current block to the previous block. Because of the computational power involved, PoW is heavily criticized for excessive energy consumption, as well as for perpetuating an unfair system where those who benefit most are those with more expensive computational equipment.

Proof-of-stake (PoS)

The consensus mechanism used on Polymesh. **Unlike proof-of-work, proof-of-sake determines which node will create or validate the next block based on how much they have staked in the system, instead of computational effort.** A stake is the number of tokens the node has for the particular blockchain. On Polymesh, node operators and stakers work together, with stakers helping node operators increase their chance of receiving rewards from validating blocks. Node operators take a percentage of the reward, with the rest dispersed among stakers, but should the node operator fail to behave reliably, they will lose their stake. This helps to incentivize honest network behaviour, since there is something (literally) at stake for fraudulent or malicious behaviour.

Nominated proof-of-stake (NPoS)

Used on Polymesh, nominated proof-of-stake is a class of PoS which defines how node operators are allowed to participate in the chain’s consensus protocol and validate new blocks. It consists of two main actors: stakers (users who stake on operators) and node operators (entities permissioned to run validator nodes). NPoS keeps the chain highly secure since it only permits node operators with the highest amounts of stake to validate blocks. This makes it harder for a single adversarial to attack the chain since it takes considerable reputation to build up stake. It also makes attacking the system costly since such behavior results in stake being slashed.

Nodes

On a blockchain, data is stored in nodes, which function like servers and contain a copy of the blockchain and its transaction history. Architecturally, Polymesh is a public permissioned blockchain, meaning any user can run a regular node or check the upholding of network rules and the public state secured by the blockchain. However, only specific entities called node operators can run the nodes that author new blocks or vote on block finality, and thereby write transactions. One of the aspects that make Polymesh unique is that operators must be licensed financial entities who meet specific criteria.

Node operators

Node operators essentially run the chain's software, certifying transactions as they are entered into the chain by validating new blocks and broadcasting them to the network. Node operators gain rewards for validating new blocks written to the chain. On Polymesh, only a set number of node operators are allowed to validate transactions, determined by how much POLYX is staked to them. Those who do not make it into the winning group miss out on rewards until the next election window (the next day). The idea is that node operators who contribute most and prove most reliable will ultimately win more often, providing incentive for good behaviour while decreasing chances of an adversarial attack.

Staking

Staking is the process of securing the network by aligning economic incentives to the correct operation of the chain through a system of rewards and penalties. It’s an important aspect of the nominated proof-of-stake consensus mechanism, which defines which blocks get written to the chain as well as the roles, rules, and incentives of the network.

Stakers

Users who back node operators of their choice with the blockchain’s network protocol token. The incentive for stakers is that they can receive rewards based on the node operator’s performance. On Polymesh, stakers bond POLYX to operators to increase their chance of winning in the hopes of receiving a cut of the reward. Should the node operator receive rewards for validating blocks, they will take a commission and the rest will be dispersed among stakers, proportional to how much they’ve staked. Staking puts the users’ tokens in a specific wallet and locks them until they choose to unbond them. A staker can be any POLYX holder whose identity has been verified through a customer due diligence process.

Block rewards and fines

The carrot and the stick that are vital to the nominated proof-of-stake consensus mechanism, and therefore proper chain operations. On Polymesh, for each block created, POLYX will be rewarded both to the node operator who created it and their stakers. However, failure to meet performance standards of the chain could lead to node operators being fined in POLYX and having their stake slashed. Ultimately, block rewards and fines provide the economic incentive to participate honestly in the network.

Sybil attacks

When one user or entity on-chain pretends to be multiple users or entities to gain more control of the network, usually to revise transaction history and indulge in double spending. Sybil attacks pose a problem for a blockchain's security since the blockchain relies on consensus. Theoretically, a single attacker can compromise consensus by controlling 51% of the network (known as a '51% attack'). Consensus mechanisms are Sybil resistance mechanisms, designed to counter such attacks and keep authoring nodes behaving honestly through economic deterrents. Identity on Polymesh is also a Sybil resistance mechanism since it prevents tokenholders from holding assets under multiple identities.

Decentralization

Decentralization refers to the level of control individual actors maintain in a distributed network. A blockchain can be considered decentralized architecturally because it is distributed across nodes and relies on consensus, but it can also be considered decentralized in terms of governance insofar as no one entity controls the network or nodes. This means no one entity can change the network protocols, turn the network off, or modify the ledger. Decentralized systems reduce reliance on central intermediaries and are argued to have better fault tolerance, stronger attack resistance, and lead to better behaviour among participants since it is harder to act in ways which benefit one while harming others.

Permissioned blockchain

A blockchain for which access to is guarded by a control layer that grants permissions to participants and governs how they will interact with the network. With Polymesh, anyone is free to join and participate in the network, as long as their identity and role are first defined and adhere to certain conditions. Polymesh requires all participants to become verified through one of its customer due diligence (CDD) providers, and requires all node operators to be known, licensed financial entities. CDD providers and node operators become approved by network users via its on-chain governance system. This improves the network's security and enables it to comply with regulations around identity while preserving decentralization.

Governance

Decentralized networks rely on governance to ensure they remain smooth, operational, and resistant to forks. **Blockchain governance is the system for managing decision-making, chain upgrades, and various other updates that guide the chain's continued evolution.** Polymesh governance is on-chain, which provides better transparency, demonstrably includes stakeholders in decision-making, and leads to greater on-chain coordination. Owing to its voting process, any POLYX holder can participate and help influence the chain. By managing network upgrades through on-chain governance, Polymesh gives all observers of the chain a clear decision on the official version of the chain and removes uncertainty for users.

Transaction finality

A strict requirement of the financial world, and guaranteed in part by technology. Many existing public blockchains rely on probabilistic finality – i.e. the assumption that after a certain amount of time (counted by a number of blocks produced in the chain), the cost of reverting a transaction would outweigh its benefits. **Yet for the blockchain to contain a true representation of ownership and meet market requirements, it must provide rapid and deterministic finality.**

Forks

The result of the blockchain splitting into two separate chains. Because of its decentralized nature, when there is a disagreement in the community (usually regarding an update), the chain can split or fork into two. Forks expose major legal and tax challenges for security tokens, especially since they lead to the duplication of assets and prevent deterministic finality. While they commonly occur during upgrades, forks can be considered more of a governance failure than technology issue since their essence is a disagreement in the direction of the chain. To counter this problem, Polymesh features forkless upgrades and an on-chain governance process to decide the official version of the chain should disagreements arise.

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. Polymath also developed the open-source code for Polymesh, an institutional-grade blockchain built specifically for regulated assets. Polymesh streamlines antiquated processes and opens the door to new financial instruments by solving the inherent challenges with public infrastructure around governance, identity, compliance, confidentiality, and settlement.

Learn more