POLYMATH

THE SECURITIES TOKEN PLATFORM

WHITEPAPER | **VERSION 3.0**

POLYMATH
THE SECURITIES TOKEN PLATFORM

Trevor Koverko*, Chris Housser†

February 2018

Abstract

A form of blockchain fundraising called an Initial Coin Offering (ICO) has existed since July 2013. Over the last two years, the ICO model has been used by hundreds of organizations to raise more than $3 billion USD. Government agencies are now analyzing the securities implications of this non-traditional form of financing, with potential consequences for ICOs that violate securities laws.

In this paper we present Polymath, a protocol to facilitate the primary issuance and to restrict the secondary trading of blockchain security tokens. Polymath uses a blockchain-based protocol that provides a suite of tools to coordinate and incentivize participants to collaborate and launch financial products on the blockchain.

By creating a standard token protocol which embeds defined requirements into the tokens themselves, these tokens can only be purchased and traded among verified participants.

1 Securities Regulation

For centuries, the regulation of securities has encountered cycles of increased regulation and deregulation. New regulations were enacted in response to a major economic disaster [1] [2] [3], and deregulation resulted from movements to ease the requirements of regulatory compliance in an effort to stimulate economic growth [4] [5].

1.1 The Bubble Act

In the early 1700s, shares in the South Sea Company experienced an unprecedented rise in price that appeared to be decoupled from their fundamental value. The founders opportunistically cashed out their shares. Investors followed suit and raced to sell before the value of the stock cratered. South Sea Company shares plunged 83% and induced what was perhaps the first global stock market crash. Around this time, an English statute called the Bubble Act was passed (June 9, 1720). The Bubble Act required companies to get a royal charter before selling shares [1]. To this day, in the U.S., companies are formed by making a state filing that grants their existence.

*trevor@polymath.network
†chris@polymath.network

1.2 The Securities Act and Securities Exchange Act

The 1920s began with many companies selling securities based on promises of large profits backed by little, or even fraudulent, supporting information. The subsequent stock market crash of 1929 and ensuing Great Depression prompted a new set of regulations which form the basis of modern securities law in the U.S. The Securities Act of 1933 [2] had two main objectives:

1. Require investors to receive financial and other material information concerning securities being offered for public sale.

2. Prohibit deceit, misrepresentations, and other fraud in the sale of securities.

The Securities Exchange Act of 1934 [3] was introduced a year later to regulate the secondary sale of securities—sales taking place after a security has been initially offered by a company. The Exchange Act also established the United States Securities and Exchange Commission (SEC) in order to enforce its provisions. The SEC's enforcement mandate has now grown to include the enforcement of, and rule-making under, the Securities Act and other security laws, including one of the most recent security laws, the Sarbanes−Oxley Act of 2002 [6], which was enacted after accounting and related scandals. Companies are responsible for satisfying reporting requirements and disclosure obligations set by the SEC or else risk enforcement action, and in some cases private litigation, for providing fraudulent or incomplete information or for violations of the many substantive and technical rules that have grown in volume over the years.

1.3 The Dodd-Frank Act

The Dodd−Frank Wall Street Reform and Consumer Protection Act [4] came into law in 2010 with widespread implications [4]. These represented a "sweeping overhaul of the financial regulatory system, a transformation on a scale not seen since the reforms that followed the Great Depression" [7] and caused compliance costs to dramatically increase. The increased costs, complexity, and annual reporting requirements applicable to public companies as a result of the Dodd Frank Act and other growth in regulatory burdens have kept even large tech firms out of the public market in recent years.

The effect of U.S. securities regulation extends beyond the country's boundaries. As the largest and often best market to raise capital, the rules and regulations governing U.S. securities are particularly relevant for many of the world's private and public companies looking to raise funds. Despite the many regulatory considerations, the integrity and confidence in the U.S. markets and safety of the U.S. dollar continue to draw capital from investors worldwide.

2 Market Context

The global securities market is composed of three major instrument types: equities, debt, and derivatives. In 2016, these three markets had total notional values of US $67 trillion, $99 trillion, and $1.2 quadrillion, respectively [8].

2.1 Primary Markets

The primary securities market allows for companies, governments, and public sector institutions to raise capital directly from investors by offering registered securities in the context of a public offering, or by offering securities under an exemption in the context of an unregistered offering. In order to sell to the public, regulators have required companies to register securities in order to (i) protect investors by ensuring public dissemination of information, and (ii) prohibit misrepresentation or other fraud in the sale of securities [9].

Should a private company decide to "go public", capital can be raised through registered offerings. This is typically done via a process known as underwriting, where an investment bank or syndicate of securities dealers determines the price of the security that investors are willing to accept, bears the risk of selling the security to the public, and profits from the spread. Follow-on offerings allow companies to raise additional funds by issuing more securities.

Companies with a combined year-end market cap of US $800 billion went public by way of initial public offering (IPO) in 2016 alone [8]. Costs related to the issuance of securities, including those related to regulatory compliance, are substantial. They typically range from 5% to 10% of the amount raised [10].

2.2 Secondary Markets

Previously issued securities are bought and sold in the secondary market. These securities include equity shares, debt, and more "exotic" instruments. Secondary exchanges such as the New York Stock Exchange provide centralized, highly liquid secondary markets for trading securities. Other secondary markets exist "over the counter", where the owner of the security must manually contact and trade with a registered broker-dealer.

The costs of transacting on secondary markets vary widely, ranging from 0.25% to 3% of the total trade amount. In 2016, global equity trading on all online order books totalled US $84 trillion and bond trading totalled US $16 trillion. Related transaction costs are estimated to be at least US $250 billion [8].

3 Private Markets

Regulatory bodies generally provide exemptions for private and public companies wishing to avoid onerous disclosure requirements and large fees related to public offerings, usually by structuring offerings so that undue risks to the general public are avoided. In the United States and Canada, these exemptions center around "accredited investors" – investors with enough financial savvy, assets, or a combination of the two to be considered competent to make their own decisions and to sustain any losses. For example, under Rule 506 of Regulation D of the Securities Act, as amended [9], the SEC allows companies to issue securities to accredited investors, subject to restrictions on marketing, general solicitation, and, usually due to other regulations, number of investors.

New regulations enacted in 2015 allow certain public offerings to be sold in small amounts to non-accredited investors without full registration. However, there are still significant restrictions on who can contribute, how much they can contribute, and the total amount the business can raise [11], as well as SEC

filings that are intended to provide fulsome information to investors but include many technical requirements and are expensive. Businesses that need access to a larger pool of investors or higher individual contributions often struggle to raise funds. Another downside of private markets is that, because their issuance has been simplified but trading has not been, they are far less liquid and have no robust market makers or price discovery mechanisms; investors may be unable to sell their shares for years, if at all.

4 Blockchain Technology

Historically, transactions have depended on processes that build much needed trust—that is, each party must offer evidence that it has the capacity to hold up its end of the bargain. If one party hands over cash, and the other party fails to deliver the security, serious market inefficiencies arise. Financial intermediaries—whether for commercial reasons or due to regulatory mandate—have blossomed in every place that market integrity is lacking, in order to provide assurances that the markets will function without undue friction. The blockchain can resolve that issue.

For the first time in history, an immutable, decentralized ledger exists on a global scale, eliminating the need for middlemen, complex auditing systems, and long settlement times. Open (permissionless) protocols mean settlements no longer depend on connecting fragmented legacy systems. Additionally, because the ledger is append-only (existing records are immutable), it provides a high degree of accountability, with blockchain timestamping built-in. In other words, a reliable audit trail is built into the technology.

The most commonly used methods for ensuring consensus on a blockchain are Proof of Work and Proof of Stake. They ensure truthful consensus by making the costs of manipulating the network greater than the profit to be made from such deceitful transactions. For example, on the Bitcoin blockchain, the cost of censoring new transactions at the time of this writing would be billions of dollars [12]. Few entities have the capability to pull off such an attack, and as the network grows, the cost of attacks increases, making them increasingly improbable.

The most popular blockchains are decentralized. Transactions are algorithmic and the security of the network is maintained by thousands of independent nodes. Block-chain systems eliminate the need to trust the operators of a centralized system. Without a single source of truth to lobby, blackmail, or bribe, the decentralized model greatly reduces the chance of regulatory capture. Blockchain technology opens the possibility of more transparent markets that are less susceptible to the control of financial oligopolies operating within a regulatory environment they have helped create.

4.1 Smart Contracts

Over the past few years, Turing-complete programming languages have been implemented into decentralized blockchains. These systems use “smart contracts” (software programs stored on-chain that are automatically implemented upon specific conditions being satisfied), to add and modify data algorithmically however a user designs it. This data extends well beyond simple account balances,

and may include metadata, account restrictions, transfer rules, as well as any other calculations a regular computer can perform.

The most widely used Turing-complete blockchain, Ethereum, grew out of a frustration with trying to implement complex logic on top of Bitcoin [13]. Ethereum simplifies the task of implementing complex financial logic on a blockchain. With only a few lines of code, smart contracts can transfer assets or establish escrow conditions to be executed algorithmically, with all the benefits of blockchains as described earlier. In other words, if two parties enter into a smart contract, and each party presents their asset, the transaction is automatically effected without risk of failure; if one party fails to present its asset, the other party retains its asset and can move on. There is no risk of payment on one side, and the failure to deliver on the other side. The smart contract can be designed to effect a transaction instantaneously, or can be designed to effect upon future conditions begin met.

4.2 Initial Coin Offerings

Recently, smart contracts have been used for Initial Coin Offerings (ICOs) or token sales. These tokens usually conform to a standard (e.g. ERC2 or ERC223, which are Ethereum-based technologies that generally allow for exchange of tokens of the same standard), which allows them to be offered for sale and trade on a number of online platforms.

The global adoption various forms of token sales an ICO fundraising structures has led to an explosion of new capital formation—whether through virtual currencies (representing a means to transfer value but not backed by other functionality or a promise), utility tokens (software that might access to goods or services, rather than being designed as a financial instrument), or tokenized securities like equity in companies—that has outpaced both the seed and venture capital investment markets. ICOs and other sales have raised US $2.3 billion to date. In 2017 alone, ICO funding surpassed US $1.2 billion [14]. Unfortunately, some ICOs have made inaccurate, and in some cases fraudulent, claims in an attempt to raise funds, which has attracted the attention of regulators in a number of countries [15] and pressed regulators to consider whether to formally bring the investor protections of securities laws or bear on the diverse universe of transferable tokens of various kinds.

As noted above, besides straightforward virtual currencies, there are, in effect, two basic kinds of tokens sold in a token sale or ICO: utility tokens and security tokens. Utility tokens are used to access services or assets, which are themselves often based on smart contract technology. The purchase of a utility token is akin to purchasing the rights to use a software or a product. These tokens are like pay-per-use SaaS offerings, subscriptions to content, or a means to compensate contributors to a platform in a manner similar to in-game currencies. As a general rule, tokens representing the sale of products are exempt from the Securities Act in the US [3], provided they do not constitute an "investment contract" as defined by the Howey Test (or otherwise meet the fairly complicated definition of "security") such that they are deemed to be a securities offering [16]. Other jurisdictions have similar regulations and common law tests to determine if a sale of a good, contract or product represents a securities offering.

One kind of security tokens represent an equity stake in an organization, or a

claim to the wealth generated by its activities. Sales or issuances of these tokens with these features tend to constitute a securities offering, which means that they are subject to securities regulations; issuers need to ensure that token sales comply with all applicable securities laws or risk severe penalties. Registrations and exemptions must be considered, and the efficient transferability of tokens that is at the core of their technology may be stifled by a regulatory apparatus that requires intermediaries and government filings of various kinds.

In contrast to traditional Securities offerings, the general public still does not have a good grasp on the truly wide range of products and technology underlying the many tokens that technologists have created, and because securities regulators are still only beginning to think about developing rules for this space, regulatory bodies have temporarily resorted to issuing warnings [17]. ICO investors are cautioned about the investment and enforcement risks of ICOs, and issuers—even pure coders who think they are just pushing blockchain's revolutionary technology advances to the next level—are reminded that they could be subject to securities laws despite their perception to the contrary. Regulators are applying increasing legal scrutiny towards token sales to ensure compliance where appropriate. Some ICOs have cancelled their offerings after discussions with regulators, while others face the risk of prosecution [18].

4.3 The Roots of the ICO Boom

The ICO boom is driven by creation of the ease of transferring value via the blockchain, excitement about this new form of selling software or engaging in fundraising, by the many investors excited by the technology, and by pent up demand induced by the current regulatory regime. The cost, complexity and delay associated with many types of existing financing options can be a significant barrier to a successful financing. Even for those who can afford the time and money to overcome those barriers and, for example, access the largest potential investor base through public offerings (IPO and follow-on offerings) may find that the ongoing reporting requirements, costs linked to this approach, and other risks may not be worth the benefits.

One of the major benefits of a public offering, broad investor base aside, is the exit opportunity it provides the initial shareholders of a company who first showed faith in its promise and accepted the risk that the company would fail. The national economy can benefit from making it easier for capital to find its most suitable target to support growth and innovation. However, due in part to the ever-growing costs associated with going public, even large private companies are often opting for alternative financing methods or growth strategies (e.g. Uber and Airbnb).

While many companies would love to be "unicorns" (private companies with valuations above US $1 billion) and obtain high levels of venture capital financing, the reality is that raising funds can be very difficult. Smaller companies are often restricted in the size of their accessible investor base, which severely limits fundraising upside and minimizes the chances of achieving a liquidity event like an IPO. This trend can cause problems for a company's employees, founders and investors. Employees' stock options are reduced in value as the chance of a profitable exit diminishes. Company owners lose out on opportunities to raise revenue in order to expand or increase their runway. Retail investors are prevented from investing in early stage, high-growth companies. And the economy

loses out on the opportunity for money to fund the most promising advances.

5 The Polymath Solution

The Polymath platform opens up the blockchain to legally compliant securities offerings with a network of services designed to lower associated transaction costs over time.

At a high level, Polymath:

1. Provides a decentralized protocol for trading security tokens.
2. Enables individuals and institutions to authenticate their identity, residency, and accreditation status to participate in a wide range of security token offerings (STOs).
3. Allows legal delegates to bid on new issuances to represent issuers on offerings to be done in a regulatory compliant manner.
4. Matches issuers with developers who can translate issuers' Security Offering parameters into secure code that generates ERC20 compatible tokens.

Polymath's system can be modeled as tools for a set of *Participants*, *Assets*, *Marketplaces*, and *Processes*.

5.1 Participants

Investors: Individual consumers or institutions wishing to purchase or trade security tokens.

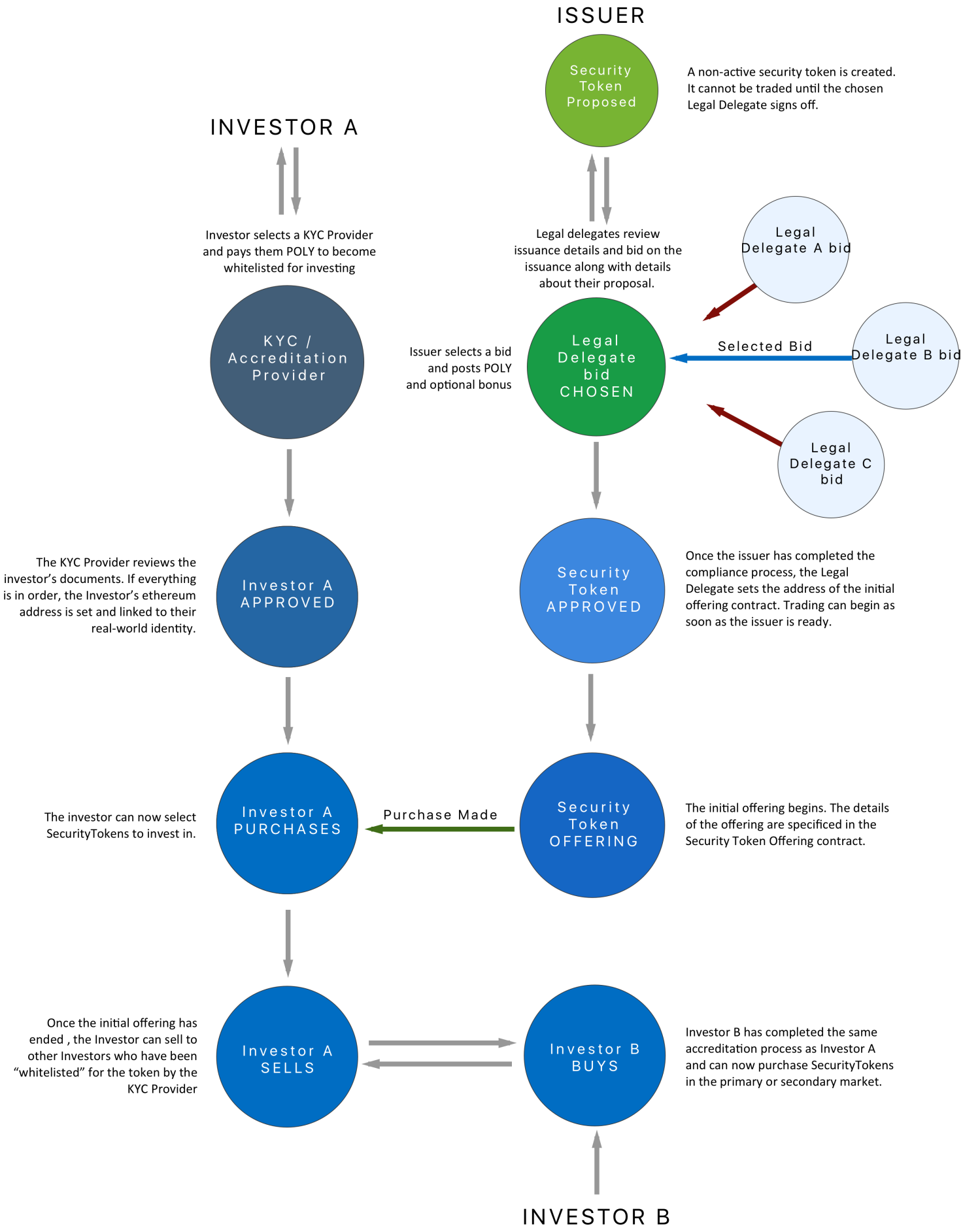
Issuers: Entities that wish to sell security tokens.

Legal Delegates: Delegates place bids, including proposals with enforceable on-chain restrictions. Delegates can also act as representatives off-chain to help guide issuers through the compliance process.

KYC Providers: In order to participate in the system, Ethereum addresses need to be matched with investors. These investors may also wish to be accredited in relevant jurisdictions in order to remove certain investment restrictions. A KYC (Know Your Customer) provider validates the real identities of participants and performs due diligence to accredit them.

Developers: Software engineers who create or review initial offering contracts for security tokens.

POLYMATH
THE SECURITIES TOKEN PLATFORM



5.2 Assets

POLY Tokens: The core utility tokens that power the Polymath system. A POLY token is a standard ERC20 token.

Polymath Chaincode: At the heart of the Polymath platform are a set of smart contracts. These serve to coordinate interactions between participants. Polymath smart contracts are deployed on Ethereum, but could be linked to other platforms.

Polymath.js: `Polymath.js` is a JavaScript library that simplifies interacting with the Polymath chaincode, as well as a set of tools for encrypting documents using Ethereum's addressing scheme and generating cryptographic proof of process artifacts (see Appendix A Encryption).

5.3 Marketplaces

All amounts in the marketplaces are denominated in POLY, and the management of escrowing and releasing fees is performed by a Polymath smart contract. This section provides an overview of each marketplace.

KYC Provider Marketplace: This marketplace matches up individuals with KYC providers who offer validation and accreditation services in their jurisdictions. KYC providers post the cost to use their services.

Legal Delegate Marketplace: All securities must go through the legal delegate process. Legal delegates help issuers complete this process and complete the steps for an issuance. For each new potential security token, delegates bid on the cost of representing that issuer during the process. The platform assumes no knowledge about the delegates, and it is up to the issuer to do their own due diligence about the legal delegate's claims and credentials. Given the nature of the transparent blockchain, third parties will be able to track the number of issuances done by a particular delegate. This added information should help issuers decide which delegate to use. Delegates are also required to go through KYC validation.

Developer Marketplace: Issuers may wish to have their Security Token Offering (STO) Contract created or reviewed by one or more smart contract developers. Developers are able to bid on these jobs.

5.4 Processes

At its core, the Polymath system is a collection of processes for managing the interactions between participants. This section outlines how securities are planned to be issued on the Polymath platform, how Polymath provides a framework for legal delegates and service providers to enable regulatory compliance in jurisdictions worldwide, and how the Polymath platform can help issuers through this complex legal process while aiming to improve the security, auditability, and accountability of the securities market.

In order to illustrate this process, in the next few sections we will walk through the primary processes we intend to implement in the Polymath system from the point of view of several hypothetical participants.

5.4.1 Investor Onboarding

Sophia wishes to invest in a security token on the Polymath platform. In order to purchase tokens, she needs to have her identity and accreditation status validated by a KYC provider. Sophia uses a web interface to view data, stored in a Polymath smart contract, about KYC providers. Sophia lives in Brazil, so she begins by limiting her search to only those providers who offer KYC services in her country. To review providers, she sorts them by cost and by the number of identities they have successfully validated. Because the smart contract also stores URLs for these providers, Sophia can review their web page and do a web search for the company, or contact them directly if she wishes additional assurances.

Once Sophia has chosen a KYC provider, she indicates her willingness to work with this provider by sending a transaction with the required amount of POLY tokens to the smart contract which manages the KYC marketplace. These tokens will be held in escrow until the process has been completed. The smart contract records Sophia's Ethereum address and chosen provider, but no personal details.

As soon as the KYC process begins, Sophia and the KYC provider can upload and review documents, and work through the KYC provider's checklist. Polymath provides a library `Polymath.js` to power secure, auditable document sharing, but does not have access to view the documents themselves (see Appendix A Encryption).

Once the KYC provider has finished validating Sophia's identity, the KYC provider sends a transaction to the Polymath smart contract specifying Sophia's jurisdiction. If Sophia has asked to be accredited, the KYC provider will note this as well.

Along with details relating to Sophia's jurisdiction and accreditation status, the KYC provider can use `Polymath.js` to produce a final hash to record to blockchain. In this way, the identity validation process can be audited at a later time, so long as the auditor is given access to the documents by Sophia or the KYC provider (see Appendix B Proof of Process). Where required by law, a security broker will be engaged by the investor and will address matters of suitability assessment, the holding of securities, and other customary matters as required in the relevant jurisdiction.

Sophia is now able to buy and sell relevant categories of security tokens on the Polymath platform. Polymath's smart contracts enforce any of the limits on her investing. This KYC validation will also be used to validate her identity and eligibility to trade in the secondary market with other investors with validated identities.

5.4.2 An Issuer Launches A Security Token

Acme Corporation wishes to sell security tokens to raise capital for its venture. It begins with an Ethereum transaction to propose a new security token. Acme's name, ticker, and other public information is stored on the chain. Should it choose to do so, Acme can use a multiple signature digital wallet for all of its transactions to make sure that the correct combination of officers are signing.

From a technical standpoint, the issuer starts this process by making a call to the Polymath `createNewSecurityToken` function, specifying the desired secu-

rity token details (i.e. type of security, rights contained in the security, desired amount to raise, company name, ticker, etc). Their new ST20 standard security token is instantly created—although not yet useful—and stored in a registrar contract on the Ethereum blockchain. The total supply is owned by the issuer and non-transferrable until the legal delegate and issuer confirm that the steps have been completed for the token to be issued.

At the point where the token has merely been created, any legal delegates on the Polymath platform are notified of this proposed issuance in real time using the event logging functionality built into Ethereum. They are able to propose legal details for the offering (e.g. jurisdictions of investors, type of offering under relevant regulations, hold time before tokens can be resold) as well as the legal delegates' bounty (see Appendix C Successful Issuances).

Acme Corporation reviews these bid details, and ensures that enough POLY is sent to the security token contract to cover the costs of the chosen bid. Then Acme and the legal delegate work together through the compliance process.

Polymath provides a web interface for sharing documents in a structured way and generating merkle hash trees from documents. Acme can choose which of these documents they share with the public. This allows the Polymath system to be used to get longevity of digital documents in a faster, easier, and more secure format than previously possible—i.e., if a security token offering is audited, the issuer can provide documents that are cryptographically signed and timestamped on the blockchain, and can explain the process which was taken (see Appendix B Proof of Process).

Once all steps of the compliance process have been completed and verified by the issuer and the legal delegate, the delegate will advise the issuer on the investor requirements (jurisdictions and accreditation flags) for this Security Token Offering. The investor requirements will limit who can hold tokens to residents of certain jurisdictions, set limits on whether non-accredited investors may invest, and place other restrictions as the issuer deems appropriate. At this stage of the issuance process, a bounty is assigned to the legal delegate, but locked until successful issuance or other event of payment occurs pursuant to the smart contract (see Appendix C Successful Issuances).

Note that each STO is its own smart contract. This contract ensures that all security tokens related to that contract are traded in accordance with any rules that result from the compliance process, and the smart contract can be updated by the issuer to reflect corporate events and the like. These contracts use the KYC registry contract as an authority on identity/address pairs. This allows investors to participate in multiple offerings without going through the KYC process multiple times, tracks that investor's limitations, and provides for the updating of the KYC process for an investor as the KYC provider deems appropriate.

5.4.3 Token Purchase Story

Sophie is interested in purchasing shares of common stock to be issued by Acme as part of its Security Token Offering. She has already completed the KYC process and reviewed the offering documentation with her financial and tax advisors, but she still needs to check that she is allowed to participate in the offering. Because the issuer hasn't blocked her KYC provider, or residents of Brazil, because Sophia has the correct level of accreditation, and because

Sophia's broker enables the transaction, she can purchase tokens.

Acme has posted a hash of all necessary documents related to the offering to the blockchain, and made the documents available online. All purchase transactions must come in with a hash of the documents. Token exchanges wishing to act as a forum where their customers can invest in the initial offering should ensure that purchasers are advised of the existence of these documents. By including the hash of the documents, investors like Sophie are affirming their understanding of the contents. `Polymath.js` includes a tool to validate that the document hasn't been altered (any alteration would change the associated hash).

5.4.4 Security Token Offering Contract Story

In order to allow more fine grained requirements in a securities offering, legal delegates work with smart contract developers to create new STO contracts. For example, if a security token requires that all investor tokens be locked up for one year after the initial offering, the STO contract is able to enforce this. STO contracts allow the issuer to have control over the offering while reducing time and cost to market by reusing existing contracts that have already undergone security audits and have been used without issue by others.

Developers who create STO contracts using Polymath tools are incentivized by the ability to earn royalties. Every time a developer's STO contract is used, the developer will receive a payout from the issuers (also locked until successful issuance or other event of payment, see Appendix C Successful Issuances). Additionally, because there is a record on the blockchain of previous STOs the contract has been used for, there is an incentive to build reputation for associated contract developers.

The issuer is able to approve the security token for initial offering by calling the `setSTO` function with a contract address, start time, and end date of the offering. The issuer also has the discretion to execute independent reviews of the STO contract and once satisfied, can transfer the security tokens it owns to the STO contract, making the securities available for sale after the start time.

5.4.5 KYC Provider Story

A KYC provider can join the Polymath network by calling the `newProvider` function with its desired fee per verification and a URL that points to a page explaining its services for Polymath users. KYC providers are notified when an investor requests verification or runs an algorithm to determine jurisdiction and accreditation status, and calls the `verifyCustomer` function to set the investor's verifications. The investor will also include a sufficient fee specified by the KYC provider that is held in escrow until a successful issuance or other event of payment.

5.4.6 Legal Delegate Story

In order to join the Polymath platform, a legal delegate sends in a transaction with its base POLY fee and details about the law firm. Among other things, it would include a URL that points to a page on its website with information about its services for issuers on the platform. This web page should also include

the ethereum address of the law firm to prove that the firm has authorized the individual lawyers to act with respect to the Polymath platform. Once on the platform, legal delegates can receive notifications when new posts for new issuances arrive, and bid on them.

In addition to their bids, legal delegates can post a bond in POLY. This bond indicates to the issuer that the legal delegate is willing to ensure the quality of its work up to some limit. The legal delegate would set an amount of POLY, how long the bond would be in force (from the time the security sales begin), and a "burn" threshold. In order to destroy the legal delegate's bond, a percentage of the total security tokens greater than this threshold would have to vote to burn the delegate's tokens. If the votes to burn exceed the threshold within the bond period, all POLY tokens in the bond are destroyed. If not, the POLY is moved back into the delegates main account and can be used for any other purpose. As the security token holders have no built-in incentive to burn the delegates' POLY, and would have to take positive steps to do so, it is expected that voting to burn would only happen if significant issues made token holders to want to strip the delegate of its bond.

5.4.7 Token Sale Story

Sophie is ready to rebalancing her investment porfolio and wishes to sell her Acme tokens. Polymath is an open protocol, meaning Sophie can visit any supporting exchange to sell her tokens so long as her broker (if required) has enabled the transaction. Each exchange will have its own rules for who may buy and sell security tokens on it; for example, in some jurisdictions, the exchanges will be limited to those that have registered in an appropriate capacity with the local security regulator. The protocol rules allow Sophie to sell her tokens to any qualified buyer, provided any hold period on the tokens has expired and no other restrictions are in place. James is a buyer in the marketplace who wishes to purchase the securities Sophie intends to sell. In order to enable the transfer of these security tokens to James, the Polymath platform exposes a public interface for any exchange to validate James' accreditation and jurisdiction status based on his public Ethereum address. Once validated, and subject to any required enabling by James' broker, a transfer to James' public Ethereum address is able to occur. The issuer's transfer agent will then oversee the automated updating of the issuer's share registry and fulfill any related regulatory requirements.

5.4.8 How Token Sales are Restricted for Purpose of Regulatory Compliance

Security tokens are different from the current blockchain model, where tokens are freely tradable after the primary issuance. Bearer securities, meaning securities that are deemed owned by whoever holds them, are illegal in most jurisdictions. Various numerical and other thresholds can, if exceeded, result in significant regulatory obligations for an issuer. Issuers and financial intermediaries owe duties with respect to tax reporting. Regulations provide protections in some cases from hostile takeovers and other actions by shareholders who may seek to acquire, control or influence a company. Corporate documents or securities terms provide for various rights as to voting, tender offers, dividends, income and other rights that must reach the relevant security holder. The pro-

vision of ongoing information to the public or the security holder tends to be required. The Uniform Commercial Code and variants in many jurisdictions have developed to provide a process by which the successful transfer of a security from one person to another has been formalized and made predictable. For these and a variety of other reasons, security tokens must trade differently from other ERC20 tokens, bitcoin, virtual currencies, and other digital assets. In addition, token exchanges generally do not list security tokens in order to avoid regulatory enforcement for dealing securities. With the advent of decentralized and even anonymous exchanges, this form of regulation becomes difficult and has caused some governments to ban token sales entirely. With freely open secondary trading, issuers would be unable to determine the identity, jurisdiction and accreditation status of its securities holders, and would be unable to comply with applicable law, with potentially major consequences for the company, its management, its security holders, and the customer base for the company's products.

Polymath seeks to solve this problem by addressing secondary markets at the protocol level withing the existing regulatory and commercial frameworks. When a security token is created and issued through Polymath, the token is programmed to verify who can buy and sell the token. The security token restricts token holders from trading to any address that has not passed the required verifications. With this baked-in restriction, even decentralized and anonymously run exchanges, such as exchanges in jurisdictions that do not impose substantive regulations, will only be able to conduct trades to authorized participants consistent with the issuer's requirements. The restrictions provide issuers assurance that their tokens will only be held by authorized investors and will be subject to those other restrictions that the issuer wishes to place on the securities.

This fundamentally changes the securities market. The need for operating and maintaining a centralized exchange disappears almost entirely because the security token is self regulating. Additionally, it ushers securities onto a new decentralized secondary market with different fee structure, instant settlement times, and around the clock trading.

6 Security, Scalability and Auditability

The document audit trail and data from the security token creation and compliance processes are uploaded to the transparent and fully auditable Ethereum blockchain. Compared with current centralized and vulnerable storage systems for securities offerings such as the SEC's EDGAR database in the United States, Polymath seeks to prevent high-profile hacks from occurring by isolating the storage of each security offering.

This all-digital approach allows for a much more efficient and scalable system, which is important given that the EDGAR system is currently processing 50 million document requests and over 1.7 million electronic filings per year [19]. Many non-U.S. jurisdictions have no similar online system with such easy access. Polymath allows for records related to the security in questions to be validated, without having to validate all other blockchain data that is unrelated, thus reducing the validation from hundreds of gigabytes of data to a fraction of that amount. For documentation that will have to be uploaded to EDGAR,

the hope is that an issuer's documentation will be easier to compile for filing purposes once the Polymath tools are utilized.

7 Polymath Tokens (POLY)

In order to power this new platform for the issuance and trading of regulatory compliant securities on the Ethereum blockchain, an ERC20 standard Polymath (POLY) token will be created and distributed to network participants. One billion POLY tokens will be minted and no additional POLY tokens will ever be minted after that. POLY tokens are the underlying economic unit of the Polymath marketplace.

POLY token allows value created in the system to be captured by the system itself. Just as almost all countries have their own currency, requiring these transactions to be in POLY sets up incentives to remain in the system. If all transactions were in ether (the native currency of Ethereum), then participants wouldn't be storing value in the Polymath platform. By requiring that people hold (and transact) in POLY, participants become subject to the same forces of incentivization that have helped ecosystems like Ethereum (and many so called "alt-coins") explode into active and diverse communities so that their products can remain viable and useful. Meanwhile, systems without their own native coin or with a "pegged" coin (e.g. Mastercoin) have struggled to develop growing or even sustainable communities or all-important network effects.

In the following sections, we describe how POLY tokens are used throughout the platform.

7.1 Issuers

Issuers are able to post bounties in POLY tokens, in order to encourage legal delegates and developers to bid on providing services towards the issuance. The size of bounty posted is at the discretion of the issuer. Highly complex securities offerings will likely require a greater amount of POLY. Factors that will determine the complexity include issuer jurisdiction, investor jurisdiction(s), accreditation requirements, and token transferability limits. The higher a bounty the issuer places, the more likely it is they will receive a wider variety of bids from legal delegates and developers. Fees will generally be payable after a security token issuance and also upon enumerated events of payment. It is possible that, over time, efficiencies could make issuance less expensive.

7.2 Developers

Developers will earn POLY for creating STO contracts. In order to incentivize developers to create security token contracts, they will be required to have these POLY fees locked up for a minimum of 3 months after the end date of the security token offering. Fees will generally be payable after a security token issuance and also upon enumerated events of payment.

7.3 KYC Providers

KYC providers pay a POLY fee to join the network. This fee is to identify legitimate KYC providers who can make this back in fees earned over time

from investor verifications, potentially even after a single successful issuance. Furthermore, they can specify a fee to be paid by each investor requesting verifications (i.e. a set amount of POLY).

7.4 Investors

Investors seeking to purchase security tokens will be required to pay a POLY fee to KYC providers for verification. Verified investors are then eligible to trade security tokens, subject to any additional requirements imposed by their broker, by issuer, or by exchanges. Additionally, where not prohibited by law, investors' payment for security tokens may be required to use POLY, but this is at the issuer's discretion.

7.5 Legal Delegates

Legal delegates are able to earn POLY tokens by (i) proposing bids on security token issuances and (ii) being selected by the issuer to take responsibility for the issuance. Along with their bids, they can specify how long they are willing to lock up their bounty.

8 Summary

The Polymath platform is designed to lower the barriers for businesses and issuers of financial products to launch security tokens on the blockchain. By introducing the tools for a simple marketplace for securities issuances and secondary trading, the Polymath platform can help bridge the gap between traditional securities and blockchain-based asset ownership and investment opportunities.

Polymath presents an open protocol for issuers, intermediaries, and participants to issue and trade security tokens, and could ultimately help usher a complex, global, regulatory landscape onto the Ethereum block-chain. If this technology can lower the barrier to entry, it could help spur economic growth and opportunities to more people and in more places than ever before.

With the multi-trillion dollar securities industry coming to the blockchain, the Polymath platform provides technological tools for individuals and companies to participate in valuable blockchain-based asset ownership and investment opportunities.

9 ACKNOWLEDGEMENTS

We would also like to show gratitude to Matt Asher, Eme Housser and David Johnston for their invaluable feedback and contributions.

References

[1] Harris, R. *The Bubble Act: Its Passage and Its Effects on Business Organization*. The Journal of Economic History Vol. 54, No. 3, pp. 610-627.

[2] *Securities Act of 1933* (last edited April 2012). Retrieved from https://www.sec.gov/about/laws/sa33.pdf.

[3] *Securities Exchange Act of 1934 (last edited August 2012)*. Retrieved from https://www.sec.gov/about/laws/sea34.pdf.

[4] Sweet, W. *Dodd-Frank Act Becomes Law*. The Harvard Law School Forum on Corporate Governance and Financial Regulation. July 21, 2010. https://corpgov.law.harvard.edu/2010/07/21/dodd-frank-act-becomes-law/.

[5] *Jumpstart Our Business Startups (JOBS) Act) (last edited April 2012)*. Retrieved from https://www.congress.gov/112/plaws/publ106/PLAW-112publ106.pdf.

[6] *Five years of Sarbanes-Oxley (2007, July)*. The Economist. Retrieved from http://www.economist.com/node/9545905.

[7] *R. Alan. Capital Markets, Derivatives and the Law*. Oxford University Press, Sept 10, 2009.

[8] *World Federation of Exchanges, Annual Statistics Guide 2016*. Retrieved from http://www.world-exchanges.org/home/index.php/statistics/annual-statistics.

[9] *Senate and House of Representatives of the United States of America in Congress (Enacted December 4, 2015). Securities Act of 1933*. Retrieved from http://legcounsel.house.gov/Comps/Securities%20Act%20Of%201933.pdf.

[10] *PwC (2012, September)*. Considering an IPO — The costs of going and being public may surprise you). Retrieved from https://www.pwc.com/us/en/deals/publications/assets/pwc-cost-of-ipo.pdf.

[11] *SEC Adopts Rules to Permit Crowdfunding*. Retrieved from https://www.sec.gov/news/pressrelease/2015-249.html.

[12] *Cost of a 51% attack*. Retrieved from https://gobitcoin.io/tools/cost-51-attack/.

[13] *Scalability, Part 3: On Metacoin History and Multichain*. Retrieved from https://blog.ethereum.org/2014/11/13/scalability-part-3-metacoin-history-multichain/.

[14] *Barnett, Chance (2017, September)*. Inside the Meteoric Rise of ICOs. Retrieved from https://www.forbes.com/sites/chancebarnett/2017/09/23/inside-the-meteoric-rise-of-icos/.

[15] *Buhr, Sarah.The SEC has charged two initial coin offerings with defrauding investors* Retrieved from `https://techcrunch.com/2017/09/29/the-sec-has-charged-two-initial-coin-offerings-with-defrauding-investors/`.

[16] *SEC v. Howey Co., 328 U.S. 293 (1946)*. Retrieved from `https://supreme.justia.com/cases/federal/us/328/293/case.html`.

[17] *Investor Bulletin: Initial Coin Offerings*. Retrieved from `https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings`.

[18] *SEC Exposes Two Initial Coin Offerings Purportedly Backed by Real Estate and Diamonds*. Retrieved from `https://www.sec.gov/news/press-release/2017-185-0`.

[19] *Clayton, J. (2017, September). Statement on Cybersecurity*. Retrieved from `https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20`.

Appendix A Encryption

The Ethereum platform can be leveraged to send encrypted messages. Ethereum addresses are based on public keys, and these public keys can be recovered from the signature of a transaction from that address (e.g. using the `ecrecover_to_pub function`). A number of tools (`bitcore-lib`, `bitcore-ecies`) can then be used to encrypt messages directly in the web browser, without sending private information over the network.

Appendix B Proof of Process

The legal process outlined in this paper generates digital documents. At times those documents may need to be audited, and participants may need to provide proof that the documents haven't been altered or fabricated at a later date. They can do so with a merkle hash tree.

In the diagram shown below (Fig. 1), one or more participants in a process create a chain of documents related to the process. They create a SHA-256 hash of each document as they go, and publish the root hash of their tree to a smart contract every time it changes. The first root hash is just the hash of *Document A*, the next one is the hash of the combination of the hash of *Document A* with the hash of *Document B*, and so on. These documents might be encrypted first using the scheme from Appendix A Encryption. However, even if participants never share the raw documents themselves, the timestamped root hashes are an audit trail which provides cryptographic proof that documents A through E existed at the time their related hashes were sent to the smart contract, and that the documents have not been altered.

It should be noted that this process works for a single document as well as a set of related documents. In particular, hashing is a useful tool for recording an immutable witness of a public document. By storing this hash on the blockchain, anyone who receives a copy of the document can hash it themselves and make sure that it hasn't been altered since it's hash was recorded to the chain.

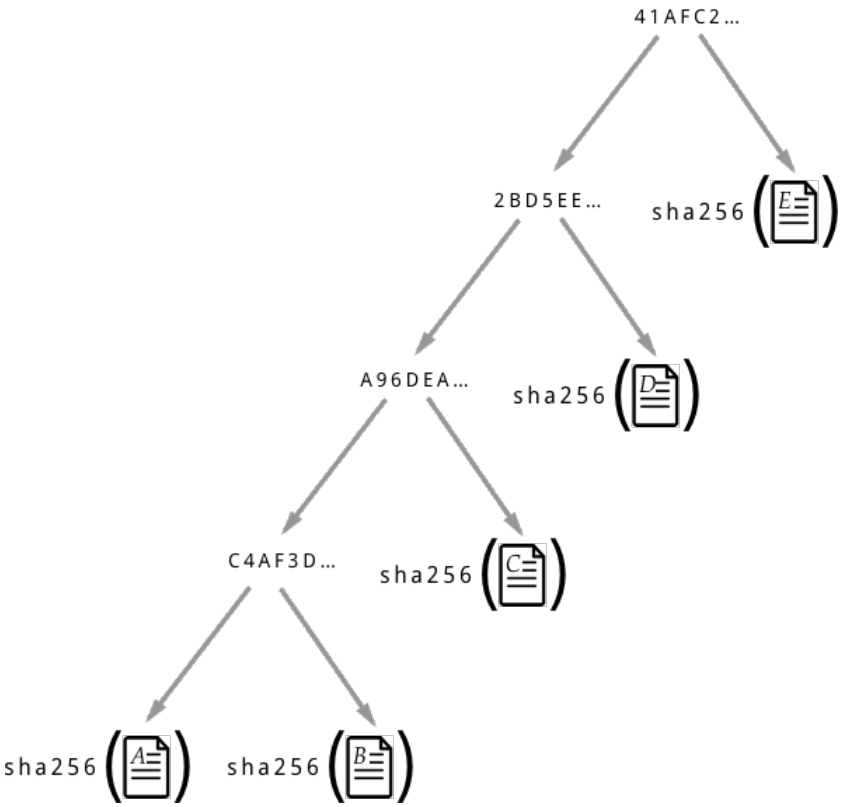


Figure 1: Keeping track of the merkle root hash.

Appendix C Successful Issuances

In order to disincentivize fraudulent activity from legal delegates and STO developers, bounty payments in POLY may be held until a successful issuance takes place or other event of payment occurs under the terms of the smart contract. In a situation where the quality of these service provider's work is in doubt, if the bounty payments are still vesting, original token holders can vote to freeze legal delegate and STO developer funds, if the issuer's token have been set up to allow for that.

This vote is calculated when an STO has ended: A snapshot of each security token holder's balances is taken and votes are weighted based on those balances. The threshold required to freeze funds would have to be specified in advance in the legal delegate and developer bids. This reduces economic incentive to attempt fraud on the network.