PROGRAMMABLE
EQUITY.NETWORK

The Programmable Equity Network
v0.3

Joel Aquilina, Sam Brooks, Anton Jurisevic, Matthew Mills,
Dominic Romanowski

September 17, 2018

Abstract

The "liquidity discount" for unlisted shares significantly reduces their effective value. This is chiefly driven by a lack of standardisation of shareholder agreements and compliance friction in the management of share ownership information. Recently, blockchains have allowed financial agreements to be made without intermediaries. Such technology lends itself to tokenisation of financial products, including unlisted company shares, as well as to the creation of markets for those assets. The Programmable Equity Network will reduce the illiquidity discount in unlisted shares by providing a single protocol for the automated issuance and trade of unlisted company shares. This solution satisfies the need to maintain a degree of transaction privacy, as well as be suitably performant, generalised, and unreliant on intermediaries.

Contents

1 Executive Summary

Unlisted private and public companies compose a large and growing sector of the economy, outperforming listed markets for growth. Yet unlisted company shares remain extremely illiquid. This is driven by a lack of standardisation in shareholder agreements; no common marketplace to exchange unlisted shares; and inconsistent record standards.

Together, these issues make exchanging shares an opaque, slow, and expensive process involving manual work by legal and financial consultants. The resulting risk and delay distorts the market. The liquidity discount imposed by this low-information environment creates mispricing of shares, obstacles to raising capital, expense and delays in share transfers, and difficulty for investors to realise profits.

The Programmable Equity Network allows for the tokenisation of private securities using distributed ledger technology. It does this by defining a common standard to allow these securities to exist natively on a blockchain. The protocol will be developed by a not-for-profit foundation funded by the proceeds of a token sale. By solving the problems outlined above, we can reduce the liquidity discount and eliminate a great deal of manual overhead. This will be achieved by the implementation of the following components:

- A set of standards for instantiating companies and shares as smart contracts to automate and disintermediate the many high-friction operations found in today's market. Reference implementations for common operations in AU, NZ, SG, and UK contexts will be provided.
- A system of asset catalogues to post assets to, and discover legally-compliant classes of shares within these jurisdictions.
- Methods of recording or proving the existence and integrity of company documents.
- A blockchain to securely operate these functions. Its associated token will be used to pay miners for executing platform operations.

Thus the Programmable Equity Network blockchain will become the source of truth for companies codifying their shareholder agreements on the platform. The extensibility of these agreements allows the creation of more complex smart contracts beyond the basic protocol, as well as novel products and services interacting with them. Because these assets are public, programmable, and secured by the blockchain, this creates a public information utility. Such a utility immediately enables a facilitator ecosystem for the supply of valuable services including KYC and investor certification, exchange listing, and document management.

The resulting open source ecosystem, built upon the automated issuance and transfer of shares, will provide a significant reduction in transaction costs, access to investment opportunities otherwise undiscoverable by investors, greater access to capital without the overhead of public exchange listing, and the creation of a novel space between listed and unlisted, allowing previously illiquid assets to be traded with greater control and transparency.

2 Background

2.1 Securities Innovation

The tokenisation of securities is the next step in the long evolution of capital markets. Stretching from the first public share issuance by the Dutch East India Company in 1602 to modern electronic trading and clearing houses, the development of capital markets has been a story of technological advancement.

Today there is a new opportunity to use distributed ledger technology (DLT) to provide the benefits of standardisation and automation enjoyed on public capital markets to unlisted company shares and enabling the discovery and exchange of securities between qualified participants. This will dissolve many strong frictions which have traditionally inhibited the deployment of private capital, unlocking powerful new capital-raising venues for unlisted companies and providing new profit opportunities to investors who would otherwise not be able to freely invest.

2.2 Obstacles to Free Exchange

There are three significant obstacles which currently restrict the liquidity of unlisted securities today:

Lack of standardisation: The proliferation of bespoke company share registers and shareholder agreements makes automation of trade impossible and introduces expensive mediators into the exchange process.

Lack of common markets: There are no common, standards-compliant market places for discovering and exchanging unlisted assets. This causes delay and difficulty in discovering counterparties and settling trades.

Poor record-keeping: Fragmented and incomplete company records make compliance, audit, fundamental value analysis and due-diligence both difficult and costly.

These three key factors increase the cost and risk associated with exchanging shares in unlisted companies. The difficulty of finding buyers in the future, delays caused by various administrative obstacles, and the indeterminate value of unlisted company shares are all factors which cause potential investors to demand a premium to compensate for these risks. This premium is substantial, and improving the liquidity of unlisted securities will eliminate significant structural inefficiency in the market that this mispricing produces.

Traditional public securities exchanges like the ASX do not suffer from these issues given the common set of exchange and filing requirements they impose, and the central platform they provide for trading these assets. Additionally, there is greater capital available for the shares listed, due to the regulator approval for retail investors to trade. Listing on public markets however is not appropriate for all companies; in order to do so, companies must relinquish significant control over the shares they issue as well as pay intermediary costs associated with listing and compliance. Small businesses may lack the scale and funding to even attempt a public listing. Furthermore, upon listing, companies and their shareholders are locked into a given platform, which means public exchanges naturally become monopolies within a given jurisdiction as all investors and companies want to go to the single biggest venue. The result is a paucity of alternative venues for raising public capital, impeding the development of some ventures.

2.2.1 Share Transfer Process

Unlisted companies currently deal with many slow and expensive friction points in the sale of these assets; shareholders often do not have the ability to simply transfer a share. Depending on the context, various complications exist, such as:

- Transacting parties must seek approval from the company to transfer;
- Companies must ensure potential buyers are permitted to own a given class of share. For example, checking that investors have sophisticated investor accreditation;
- Investors must agree to bespoke agreements, which can be costly if legal advice is sought; and,
- Companies and regulators must maintain their share registries.

To date, these processes have been overwhelmingly manual, introducing errors into documents, registries, and causing mistakes or omissions in counterparty compliance.

2.2.2 Information Deficit

The foregoing issues are exacerbated by the poor flow of information in the market which makes it difficult to break into, and impedes accurate valuation of assets within it.

2.2.2.1 Concentration of Private Capital

Existing market participants possess greater access to information, capital, and connections. These highly powerful venture capitalists preclude other investors from participating , and the result is a less efficient and less competitive market. This lack of structured marketplaces makes it difficult for buyers to find investment opportunities, and thus for companies to raise capital. These dynamics increasingly concentrate information, profits, and control within a small set of existing venture capital firms, angel investors, and brokers. This restricts access to capital, particularly for riskier ventures.

2.2.2.2 Unreliable Price History

A lack of easy access to historical share price information for unlisted shares makes future valuation a fraught enterprise. This compounds risks not just because a buyer does not have a reliable way of determining previous valuations, but they are not able to determine how readily they will be able to resell their shares in future. Reduction of the liquidity discount is not only a matter of increasing liquidity, but also of allowing market participants to correctly assess how liquid and volatile the market for a given asset is.

2.2.2.3 Inadequate Record Keeping

The condition of unlisted company records is frequently very poor, and means that shareholders and companies are often unable to correctly determine who owns what, and with what rights. Poor record keeping is also a strong impediment to investment if relevant financial data is unavailable for potential investors, while being difficult for a company to prove that such records are accurate for the time they address.

2.3 The Necessity of Liquid Private Securities

Globally, there is an excess of capital going into ever-increasingly oversupplied public markets. At the same time, private companies are requiring ever more capital in order to finance and support their growth. The problems outlined above are the primary impediment to connecting this excess capital to demand from private companies. If they could be solved, returns on capital could improve, and the global savings glut be partially ameliorated. Therefore we present the Programmable Equity Network as a solution.

3 Programmable Equity Network

3.1 Solution Overview

We propose the development of a new public distributed ledger system designed to improve liquidity for unlisted securities. This new system, called the "Programmable Equity Network", will implement standardised rulesets for instantiating companies and shares as smart contracts. The Programmable Equity Network will be built by a newly established not-for-profit foundation, with key mandates to develop:

Protocol: Open standards necessary to enable interoperability and automation of unlisted shares.

Facilitators: Fostering the development of on-ramps, exchanges, and other services that improve overall network utility.

Network: The public blockchain network upon which these standards and facilitators will operate.

The solution will emphasise:

- Standardised rulesets for the creation, customisation, and management of assets and asset catalogues in particular jurisdictions.
- An ability for shareholder agreements to be constructed from these rulesets and deployed onto a public distributed system.
- Discoverability of securities, allowing for segmentation of markets and portability of assets between them.
- Automation of trade and governance, providing open source reference implementations.
- Clear and transparent ownership and financial data accessible to both the market and regulators.
- Protection of private and commercially-sensitive data.
- Satisfaction of securities regulations including KYC/AML and sophistication requirements.

3.2 Scope

As an open system, anyone is free to build compliant service businesses on the protocol, however initially the foundation will only develop a single asset type in a fixed number of similar jurisdictions.

3.2.1 Asset Types

The protocol will initially deal with shares in Australian private and public unlisted companies, or the equivalent in other jurisdictions. This strategy will develop the largest and most important market while building out the technical infrastructure that can be readily extended to related asset types in the future.

3.2.2 Jurisdiction

The Foundation's initial focus will be on the following similar jurisdictions: Australia, the UK, Singapore, and New Zealand. This will involve developing a family of standards to implement

common functions found in shareholder agreements within these contexts. Australia has been chosen as the launch market due to its mature and highly regulated securities environment, the existence of existing facilitation services there (myStake), and the favourable ratio of market size to security tokenisation competitors. If the Programmable Equity Network can succeed in tokenising shares in our chosen jurisdictions, it will be very well-placed to move into additional markets with looser regulatory schemes.

3.2.3 Facilitation Services

The foundation will work to provide the minimum necessary services for the network to operate. This includes close development cooperation with local on-ramp services such as myStake, and partnership with other firms for exchange and IPO services. As the protocol is open, the tools exist for anyone to build new applications. Once a core set of services, businesses, and investors are using the platform, this service market will become self-sustaining, growing organically into a mature ecosystem. See Appendix A for details of how existing myStake share tokenisation functionality will be integrated into the Programmable Equity Network.

3.3 Platform Benefits

3.3.1 Diminished Administrative Burden

That most private company shareholder agreements are bespoke is a barrier standing in the way of their efficient exchange. Each agreement must be individually examined by lawyers and accountants, as their consistency, and the obligations of prospective buyers or sellers cannot be taken for granted.

The necessary careful examination of agreements and satisfaction of discovered conditions is an impediment to rapid transfers. If a common standard for shareholder agreements was known, then compliant agreements would not each require the same level of rigorous auditing. Building them as executable specifications would further speed up the process of ensuring the terms of the agreement are complied with, without having to involve expensive consultants.

By adopting these standards, companies and their stakeholders can automate the process of issuing and administering shares, slashing legal and accounting overhead. Companies will be able to see with greater clarity the terms of their own constitutions as well as who owns what shares. Due to the programmability of the assets, companies are granted much greater control. With an established set of transfer rules, the information can be recorded reliably on-chain as well as ensure companies retain total insight into all trades being executed on their shares, including the ability to programmatically challenge or intercede in those transfers. Shareholders and investors will have improved clarity over their obligations and compliance requirements given automated and cryptographically-secure auditing tools. Finally, share transfers inherit the ability to become instantaneous.

3.3.2 Improved Market Efficiency

The protocol defines a unified standard for grouping contracts into classes that comply to common interfaces. Such a protocol enables the easy discovery of assets (such as shares of a given class within a given jurisdiction), as well as satisfy the on-chain compliance steps for trading that class of shares. These asset catalogues can be run by anyone, and will frequently be the starting points to more extensive exchange and compliance service providers, such as regulators (for example for verifying that a share contract belongs to a legitimately registered business), accountants, auditors, and others.

The Programmable Equity Network's open standards will liberalise unlisted securities markets. This will open up new venues to trade for unlisted securities, providing greater access to capital and opening these opportunities to a wider population. By deploying open standards on a public distributed infrastructure, we can foster an ecosystem which provides for unlisted shares the benefits of publicly-listed shares, but with fewer downsides. The associated reduction in risk and trade friction will unlock the potential of private companies, accelerating their development, and broadening the distribution of the profits they make.

3.3.3 Enhanced Asset Liquidity

Existing token specifications such as Ethereum's ERC20 standard allow the unfettered transfer of tokens between all parties. Instantaneous settlement (consideration for the sale of assets) and a reliable on-chain share register have significantly enhanced the exchangeability and convertibility of these cryptocurrencies, and thus their liquidity. Yet this is not entirely appropriate for securities which are regulated and must abide by the applicable law and regulation governing their exchange. Such securities usually contain bespoke logic, including first purchase rights, ownership restrictions, drag-along stipulations, transfer veto rights, and a multitude of others. Performing operations like these and notifying all relevant parties in an automated way can eliminate a great deal of delay owing to manual administration work.

In sum, many securities require manual intervention before transfers can legally take place. Smart contracts allow these steps to be enforced by construction, in a more efficient manner, allowing for improved exchange. Encoding compliance requirements into a smart contract clarifies the legal requirements, enhancing process visibility, and reducing communication overhead between transacting parties and the company issuing the asset being transferred. The ability to pre-approve parties coupled with the various benefits from greater transferability and divisibility of DLT-based tokens will enable near-frictionless transfer of assets.

By distributing the source of truth for shareholdings, and enabling an openly programmable platform to operate on these cryptographic assets, we enable the possibility of asset portability through the use of atomic swap smart contracts. This means that anyone can move their asset to other blockchains and liquidity venues, so long as the rules of the original smart contract remain satisfied. This includes the listing of a single asset on multiple exchanges at once, a situation which traditional public exchanges largely preclude.

3.4 Share Contracts and The Law

Just as legal contracts can be translated into different languages for counterparty comprehension, we can similarly define source code to constitute binding agreement between parties. Such source code, along with its as-deployed on-chain location and director signatures, can be embedded directly within shareholder agreements. Thus, certain aspects of a company's shareholder agreement can be replaced with a computer program. The code itself can be legally binding whilst being accompanied by natural language explanations within the shareholder agreement so that non-specialists can understand the terms of the agreement, even as they are bound by its operation upon the blockchain.

While the Programmable Equity Netwrok will provide a standard framework of functions that can be used to construct a share contract, their associated natural language clauses may differ based on jurisdiction. For this reason the Foundation will initially only provide reference clauses for the context of Australian private company shares. In this way, shareholders may always consult an English representation of their shareholder agreement in order to make legally-binding decisions, but let the code execute to perform actions themselves. Facilitators may also wish to change the reference clause when providing on-ramp facilities such as share contract construction. Ideally the process of generating an English representation from a particular smart

contract, or vice versa, would only require a legal audit once, and thus all future instantiations of such shareholder agreements could be trusted by parties entering into them without a re-audit.

The Programmable Equity Network blockchain will therefore be the agreed source of truth for company share registers as deployed on the platform. In addition, where the contract specifies, the codified components of the shareholder agreements as deployed on the platform will be the source of truth for agreement. In the case of dispute or differences in interpretation, the code takes precedence.

These smart contracts, executed on a blockchain, automatically provide reliable audit trails for share ownership. Issuing companies may also provide reliable proofs of their documents by uploading information or information hashes to the chain for further integrity and visibility.

3.5 Application Ecosystem

The protocol is by design a low-level engineering description of general interaction patterns for participants in the network.

To allow a general audience to fruitfully interact with this protocol, we anticipate a number of on- and off-chain services to be offered by external businesses operating on the network. These businesses we refer to as *facilitators*, and they exist to smooth protocol interactions without businesses having to touch the blockchain directly. Such facilitators may not just provide their service, but will likely also handle obtaining and expending tokens on the behalf of the businesses they serve. In this way facilitators allow external actors to access the underlying protocol in a way that is both convenient and transparent, allowing them to engage with familiar terminology and constructs.

The Foundation will work to identify all necessary interaction points in the process of managing securities using the protocol and support the development of these third party products and services. Anticipated facilitation services include:

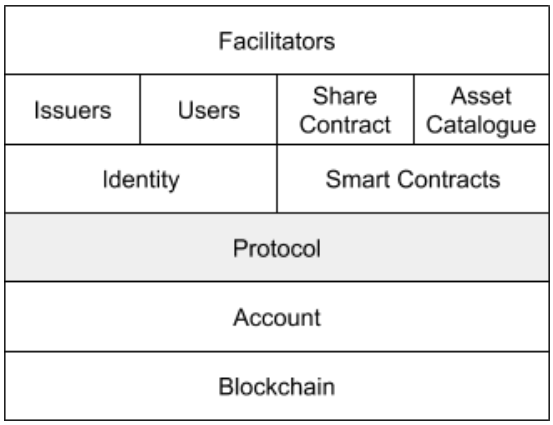
- Share tokenisation and platform on-ramping.
- Asset discovery and filtering via on-chain asset catalogues.
- Centralised or decentralised exchange platforms.
- Record-keeping, document storage, and proof of existence.
- Shareholder management, disclosure and communication services.
- Company audit and compliance services.
- Investor accreditation, KYC/AML, IPO advisory.

Each of these services has an on-chain component, and many of them are assisted by the existence of on-chain asset catalogues which operate like tags and provide the facility to prove on the chain that a firm has some property on chain, such as being a properly-registered australian company, belonging to a given exchanged, providing documents in a given format, or complying with a certain standard.

Detailed information of several of these facilitator categories are provided in later sections.

3.6 The Network

We refer to “The Network” as a the combination of a number of distinct elements, represented here as a stack:



3.6.1 Public Blockchain

The Programmable Equity Network will run on its own customised public blockchain, forked from existing, proven technologies to reduce risk and expense, and to improve reliability and security. By having a distinct blockchain network, we gain control over the following properties:

- Scalability and customisation of network operations.
- Tailored permission and security regimes.
- The addition of privacy-specific primitives to the underlying chain.
- The ability to introduce regulation-specific operations, such as regulator nodes as first class citizens.
- Easier upgradability of the protocol and for companies to update their own logic.

Given the need to ensure that any shareholder agreement is representable on the platform, the Programmable Equity Network's blockchain will support arbitrarily complex smart contracts. The capacity for miners[1] to execute arbitrary computations will also allow for the construction of on-chain services, and the securitisation and automation of different assets in the future.

3.6.2 Protocol Standards

The protocol is a collection of standardised functions that can be modularly composed to create legally-compliant, yet customisable smart contracts to replicate the functionality of existing shareholder agreements. At a fundamental level, these standards form a communication protocol that allow the interoperability of network actors to discover and interface with share register contracts deployed on-chain.

The protocol is separated into two layers: a low-level, primitive layer that provides the basic data objects (such as accounts, identities, assets and companies) for supporting higher-level, standards in a hierarchical fashion. These higher-level functions represent implementations of all common clauses found within shareholder agreements for our chosen jurisdictional context of AU, NZ, SG and UK. Appendix A discusses how on-ramps can provide convenient user interfaces to allow companies to compose compliant shareholder agreements with code from these modular protocol components.

Clearly, different rules surround the transfer of assets based on the nature of the asset and its jurisdiction. Over time the set of rules within the protocol will be expanded to incorporate

[1] Miners in this context are consensus-participating network nodes. We anticipate the use of an efficient BFT consensus algorithm over proof-of-work.

additional asset types and additional jurisdictions, however as a first step, the Foundation will focus on the shares of unlisted public and private companies within Australia.

Further detail on the initial protocol implementation are provided in Appendix B.

3.7 On-chain Identity

3.7.0.1 Accounts

An account is an identity primitive on the platform. It contains a unique cryptographic key-pair, a balance of native platform token, and a general memory store. For any message that is signed by a particular key-pair, under the assumption that the private key is held secret, there is cryptographic certainty that the message has originated from that account within the address space.

3.7.0.2 Identities

By using standardised locations for relevant fields, identifying information can be efficiently checked. Identities within the system have an explicit schema for the information they need to provide. These fields can be encrypted to protect the privacy of the users and prevent anyone without the correct key from accessing a user's private information.

Each identity is associated with a uniquely identifying address and PET token balance, as well as cryptographic capabilities for signing and encrypting messages and data, and a local on-chain storage namespace for information relevant to the individual in question. The specific information depends upon who the individual is and what they need to accomplish. The protocol defines canonical locations for common or important pieces of information, and standards for encrypting them if they must be kept private.

In this way, name, contact information, public keys, signed sophisticated investor certifications, and other protocol-relevant information can be transmitted securely and efficiently between interested parties.

On-chain Identity

Public Address:	LP123456789...
Name:	⟨salted hash ⟩
Address:	⟨salted hash ⟩
KYC:	⟨document hash⟩
Accreditation:	⟨document hash⟩
Location:	⟨salted hash ⟩
...	

3.7.0.3 Users

Entities that can own assets have protocol-defined identities. These people include investors who own and exchange assets. An account possesses its own memory space, into which a user may insert any information they wish. The system defines certain flags that a user may activate to identify themselves as a company, an investor, or another protocol-defined account type. Users may also allow others to set fields in their own address space, in an area they themselves to not control. For example, a facilitator such as an accountant may verify that they are a sophisticated buyer by providing a certificate with an expiry date. Users may also associate code with their account; the platform will provide a process to allow this code to be updated if required, or alternatively locked to updates if it must be immutable.

3.7.0.4 Issuers and Companies

The protocol pre-defines a number of identity types that are associated with key entities in the issuance and trade of shares. By way of example, the "Issuer" identity type, which is the primitive of a Company type. Issuers have an associated set of ledgers in their account memory space, which is inherited into the company identity. The company may then attach both smart contract code and ledgers associated with shares it issues. Multiple ledgers can be attached to a given company to represent multiple share classes. Further details are provided in appendices.

3.7.1 Smart Contracts and Registers

3.7.1.1 Share Registers

A company has the ability to deploy its share registers on the platform. Each share class created on the protocol will have its own associated ledger, implemented within a unique share register contract. Where these on-chain ledgers are used as the source of truth for shareholdings, the shareholder agreement will explicitly state this. As this takes place on a blockchain, the balances and actions of each shareholder's address will be public (see Settlement and Privacy).

3.7.1.2 Register Contracts

Smart contracts deployed by a company identity on the platform are known as *register contracts*. These are the on-chain components of a company's shareholder agreement. These smart contracts implement the required functions for the management and transfer of shares for a given company. Because the functionality of share contracts can vary widely depending on how the issuer wishes to manage the transactions, the company may elect to use some combination of standards as defined by the protocol for maximal automation and interoperability.

The most important functionality of the share contract is the *transfer* function. It defines the rules surrounding the handover of shares from one user to another. This can range from a fully manual process, where the issuer needs to approve every aspect of the transaction, to a fully automated process where whitelisted investors can trade the assets freely. Rules on the transfer of shares between identities on these ledgers are automatically enforced according to the logic in the associated share contract, including requiring approval from the company secretary. The logic of the share contract codifies the shareholder agreement in executable form thus making it impossible for any entity to violate the contract.

Because the share registry is deployed on a blockchain, it allows all share transfers and other operations to be permanently and immutably recorded for purposes of automated audit.

3.7.1.3 Asset Catalogues

Asset catalogues are a system of asset postings that allow company share registers to be categorised and discovered by anyone. The system will be generalised to allow anyone to set up their own catalogue, where individual catalogues set their own criteria for acceptance.

To begin with, the Foundation will create an initial catalogue where only registered Australian company shares will be posted. Validation will encompass several steps: the Foundation will firstly ensure the company is a legitimate organisation registered with ASIC, before a KYC process is be undertaken to ensure that the user attempting to post the company's assets is authorised by company executives, and finally that the company's shareholder agreement has been updated to match the associated share contract.

Posting a company to a catalogue is not exclusive; a single company can exist on multiple catalogues. For example, there could be a tech related catalogue, crowdsource funded catalogue, and so on. The catalogues themselves will be tracked by the protocol so that a user can enumerate all shares registered on the platform.

Given the desire to create a public data infrastructure, no restrictions are placed on which identities can instantiate companies. This however can lead to issues associated with fraudulently claiming to have a registered company within a given jurisdiction. This issue however will also be managed via asset catalogues who will be able to approve postings, including the ability to perform checks for each company or asset attempting to be catalogued. We foresee that the reputation of individual asset catalogues will determine which assets investors engage with. The foundation will work to ensure there are credible asset catalogues operating within important jurisdictions, to ensure the overall trustworthiness of companies catalogued on the platform.

3.7.1.4 Contract Monitoring

To provide ease of transparency to stakeholders, on-chain company communication will be publicly viewable through an event emission mechanism embedded in all smart contracts deployed on the platform. On-ramps or other services are then able to provide user-friendly interfaces to view these event emissions. Users can search through the events themselves or have the on-ramp send push notifications to their local device whilst monitoring for certain actions on-chain. This also has the added benefit of auditable records of notifications which may come in handy for potential shareholders to see what the company has been doing in the previous years or if any legal issues arise where a record of actions is required.

3.7.1.5 Messaging

Where private communication is needed, the platform has the capability to for an account send custom encrypted messages to any other account. As with other functions, this functionality can be used directly on the platform, or through the use of Facilitator or other open source software.

3.8 Programmable Equity Network Token

The platform runs on an underlying token, used to reward miners for performing and securing all general and protocol-defined computations. We will refer to it as the Programmable Equity Network Token (PET).

While the goal is to create a public single source of truth for unlisted securities, there is no ability for any one market owner to form a monopoly and extract rent from its users. We refer to this as the 'rent-extraction imperative', which exists for companies with a fiduciary duty to their shareholders to maximise profits. In our system, ownership of the network is represented by ownership of the token, meaning that the 'owners' of the network are the same as the users of the network. This allows the system to fundamentally minimise its costs (no rent-extraction imperative), while the governance can be made democratic for the good of the users of the network, and the mutually-created value can be mutually retained. This is the purpose and design imperative of the token: to stimulate the development of a public information infrastructure as a public utility.

The token is used for four purposes, split into core operations and secondary uses:

Core operations

- **General blockchain operations**
  Including, the execution of share registry functions such as share transfers and enforcement

of logic within the share registry, upgrading smart contracts, deploying other (non share registry) smart contracts and protocol token transfers

- **Protocol-specific operations**
  Including, deploying a new share registry, deploying a new asset catalogue, setting a sophisticated investor flag and token issuances

Secondary uses

- **Facilitator payments**
  The token may also be used for payment of second-level services with on-chain components, described in the facilitator section. Whenever any operations are performed, a fee is negotiated between the party requesting that operation, and the Facilitator performing that service.
- **On-chain settlement**
  Settlement is an available use for the token. Companies that permit settlement for their shares in PET allow for immediate, automated on-chain settlement. Both parties agree to transact in PET and manage their own exposure to the exchange rate to fiat currency. In the medium term, the Foundation will model standards for claims to cash held in escrow to be used as a fast-payment alternative.

3.8.1 Network Effect and Token Value

All value in any asset is fundamentally derived from a network of participants with mutual beliefs. Regulated assets derive their value from existing markets and utility that has been established over time. Crypto-assets, or tokens, on the other hand, do not benefit from this long history, and as such are still subject to massive volatility due to speculative worth. Instead, the value is derived from a network of participants who collectively agree on what value the token represents. Similarly, the value that the Programmable Equity Network brings to these participants can be defined as; the accurate pricing of assets posted to the network, the liquidity the network provides to those assets and the reduction of time spent in transferring those assets.

All network participants both provide and utilise network value according to how they interact with the network. For example, a company that requires funding utilises the value of the network by enjoying fairer pricing and greater liquidity of their shares. At the same time, the company is providing more investment options for investors.

Even though there is some cost associated with an actor interacting with the platform, as the network effect grows, this cost becomes far less than the benefit received from participating in that network. For example, consider a single shareholder and a single investor. If the shareholder must sell their assets quickly, they may be forced accept an investor bid below a fair market price. Conversely, an investor who wishes to purchase a particular company's shares may be forced to pay a similarly unfair premium to a shareholder.

By introducing more shareholders and investors, asset pricing becomes fairer. This benefit attracts additional users to the network, further reinforcing network effect and token value.

3.9 Settlement

For the Australian context, the settlement information for all share trades is reportable to the regulator. Applying this requirement to our system, we design our system to be able to record this information on chain. The protocol will define certain information to be recorded per the requirements of the relevant jurisdiction (initially, Australia) for unlisted company share transfers. For Australia, this includes: share class code, shares increased by (number), shares

decreased by (number), total number held, total paid on these shares ($), total unpaid on these shares ($), fully paid (y/n), beneficially held (y/n), top 20 member (y/n).

Where settlements for share purchases occur off-chain, companies that have deployed their registry on-chain will need to add that settlement information as a separate process. Indeed, this requirement would be written within the shareholder agreement.

Clear trade and price history of share transfers will foster greater efficiency in due diligence undertaken by auditors or investor examining the company; the information is readily accessible via the platform (under that particular company's address space), ultimately enhancing liquidity.

3.9.1 Privacy

There are many considerations in attempting to satisfy privacy and regulatory requirements of settlement information on share transfers. In particular, details such as total amounts paid (or unpaid) in consideration for share purchases, the frequency and latency of this information is typically commercially sensitive. For the Australian context, the following broad requirements exist:

- Listed (public) companies: settlement published after a period of time as determined by the exchange or regulator (on the ASX, this period is 3 days).
- Unlisted public companies: changes to share register do not need to be submitted, but may need to be provided on request.
- Unlisted private companies: settlement to be submitted to ASIC within 28 days.

The Programmable Equity Network focuses on unlisted companies and provides the ability for companies to hold pending transactions on behalf of the seller (one of its shareholders) and the buyer. In this way we can ensure a (configurable) delay is able to be achieved in the publishing of share transfer information, including settlement information. Off-chain messages from both the buyer and seller must be signed for it to be a valid transfer. Future iterations of the platform may include more sophisticated cryptographic techniques.

If privacy is not a concern to all parties involved in the transaction (the buyer, the seller and the company), then settlement may take place instantly in PET, or be immediately published as a pending transfer, awaiting acceptance by the seller after funds are received via some other means.

4 Facilitators

Facilitators are external agents who provide products and services for a general population to interact with the system.

4.1 On-ramp service

On-ramps are convenient gateways for companies to deploy and monitor contracts on the network. They provide general user interfaces for users and companies that do not want to deal with the intricacies of direct blockchain interaction.

4.1.1 Tokenisation

The tokenisation process involves digitising the company share registry and sections of the shareholder agreement. In the case where a new company is being established, these objects can be instantiated on the platform without any need for conversion. This involves the creation and deployment of registry contracts onto the platform, converting the member registry into a protocol-compliant tokenized version. New registry contracts will be able to be constructed from a library of standard clauses, have custom code, and take into account the relevant jurisdictional rules. For all existing companies, this will necessitate the acceptance of a new shareholder agreement with programmable clauses.

4.1.2 Regulator Notice

By having all this company data in one place, these on-ramps are naturally in a position to also manage company regulatory compliance. For example, within the Australian context, we expect on-ramps to integrate with ASIC to ensure all necessary compliance actions have taken place before the transfer of shares can occur.

4.1.3 Ongoing Management

Once a company has been deployed on the platform, general management of their registry contract can still be facilitated through a facilitator with on-ramp capabilities. Management functions could include pushing relevant real world data onto the blockchain, or using the on-chain information to publish updates to third parties, such as regulators. On-ramp functionality may also include visualisations of data on-chain, including a block/transaction explorer, price and volume graphs of share transfers, capital tables and any other useful company and shareholder information.

4.2 Exchange service

Exchanges are a necessary feature the network as they drive the discovery of assets for investors, buyer and seller interactions, and to facilitate trade. This includes both the listing of assets as well as providing options for settlement between parties. In the simplest case, when a trade has been submitted and accepted, the exchange may offer escrow services for fiat currency settlement. Once escrowed funds had been sent to the seller, attestations of settlement can be made by the exchange and the seller and be sent to the company for their records.

In many cases, share transfers are only permitted between accredited ("sophisticated") investors. For these restricted transfers, the registry contract will only permit contract execution where the buyer has appropriate identification and accreditation flags on their account. Note that the

responsibility to satisfy these requirements rests with the company, and so the registry contract will check the account status of the buyer against an internal authority ledger of whitelisted verification providers (accountants). If the company has whitelisted the authorising party, then the trade can complete.

4.3 Certification service

A system of KYC and investor accreditation checks for ensuring individuals are who they say they are on the blockchain will be a valuable addition to the network. By having companies trust accountants on chain, or a verified network of accountants, all investors who are accredited through those accountants can be whitelisted to trade shares without having to continuously re-prove their identity and accreditation status. The use of these whitelists is on a contract by contract basis, as the due diligence is the responsibility of the company itself.

4.4 Validation service

Catalogues act as the intermediaries between the on-ramps and exchanges. They are responsible for the validation process required to check that a company that is attempting to list on an exchange is valid, and under what criteria the company falls.

A company looking to list on an exchange, or a group of exchanges can look at the associated catalogues, to see which general criteria they meet. They would attempt to post onto a catalogue, paying a fee for the validation that they are a real company, and governed by the real directors. Along with that, depending on how strict the criteria for posting is, there could a more stringent process involving auditing and similar. In the initial stages, the on-ramps would have their own catalogues, from where partnered exchanges would gather the shares on the system.

5 Future Work

With this version of the whitepaper for the Programmable Equity Network, we have covered the key problems associated with the liquidity discount, and the major elements of the solution. Here we leave a number of elements to be explored in future iterations.

Cryptographic Settlement Timers

More sophisticated signing protocol for the delay of settlement information being written to the chain (currently, the company simply holds the transaction for a period of time before submitting it and updating the register).

Tokenised Cash

Adding a new facilitator for cash to token and token to cash liquidity, allowing for instant token settlement in real world cash.

Atomic Swaps

Atomic swap smart contracts are a method to represent the assets from one blockchain on another. The Foundation will seek to extend to protocol to include this functionality.

Disputes

A discussion on how disputes are handled, in short:

- Company has final word in regard to transfers
- If there's an issue beyond that, it needs to be dealt with in court

Document Records

The blockchain allows companies to lodge traceable records of past documents, such as financial records, audits and relevant investor information. This would give companies the ability to integrate software packages into their regular financial reporting as extensions to the Programmable Equity Network.

A Facilitator Case Study: myStake

The Foundation will seek to partner with new and existing companies to help foster a facilitation services ecosystem for users of the protocol, and this section outlines the key processes involved for a new company to list on the Programmable Equity Network via an on-ramp facilitator. myStake is a real-world example of such a facilitator, which already provides validation and on-ramp services, including share register management and regulator reporting. By extending their offering to integrate into the Programmable Equity Network, myStake's customers will be able to create smart share contracts and benefit from the protocol's facilities.

A.1 Company Tokenisation

Bob wishes to create a new software company in Australia, called *ShellScriptHeavies*. Being a brand new entity, ShellScriptHeavies (SSH Pty Ltd) has no existing digital share register. Bob signs up for an account with myStake and is provided a convenient software tool to be guided through the process of (i) establishing a new company in Australia (ii) creating a crypto-digital share register and (iii) shareholder agreement.

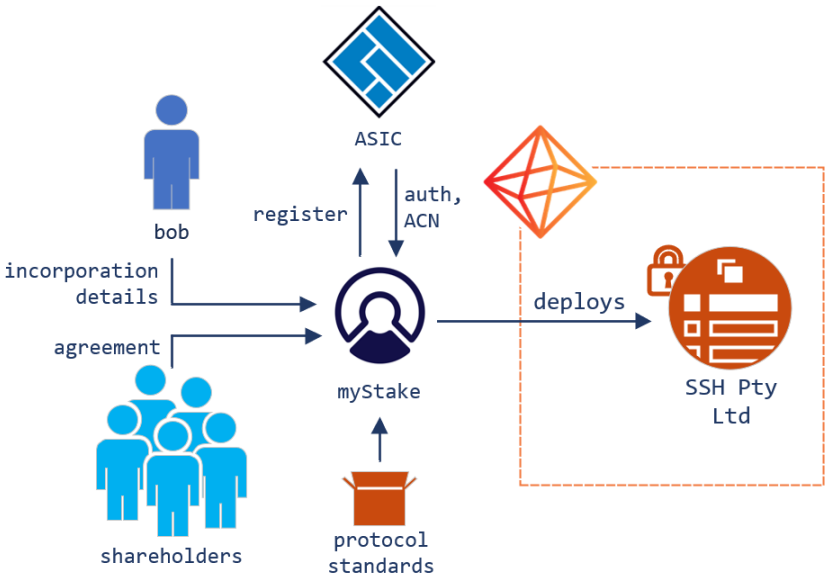


Figure 1: Using myStake to register a company on the Programmable Equity Network

myStake provides the tools to establish the entity with the regulator as well as construct protocol-compliant registry contracts to be deployable on the network. During this process myStake provides options for company shareholding rules to be enabled within the contract. In this case, the Bob wants to achieve a frictionless share transfers for ShellScriptHeavies, and so he specifies that the company pre-authorises in the contract that anyone may buy and sell shares after having been approved by the company. This includes no first rights (preemptive rights) for existing shareholders. Once the shareholder agreement is agreed to by all relevant shareholders, it can be deployed onto the blockchain. In our example, whenever the company performs authorised actions, myStake provides the interface, but the company representative (company secretary) cryptographically signs the transactions using a private key stored offline.

myStake instantiates the share contract with the issuer being the company, as well as issuing share holdings to all existing shareholders. For shareholders who do not have a private key,

myStake automatically generates accounts, including their balances and private keys, on the network. myStake then sends a notification to all unregistered participants to enquire whether or not they wish for myStake to continue to hold their keys.

A.2 Asset Posting

Once the company is on the platform, myStake prompts Bob to now post his assets onto one or more asset catalogues, making it discoverable and providing greater exposure for the assets to investors. myStake suggests a number of catalogues, including its own: "Australian Unlisted Company Catalogue". Bob agrees to the posting. Once catalogued, all exchanges that are subscribed to that asset catalogue will know about the new company and shares on the protocol.

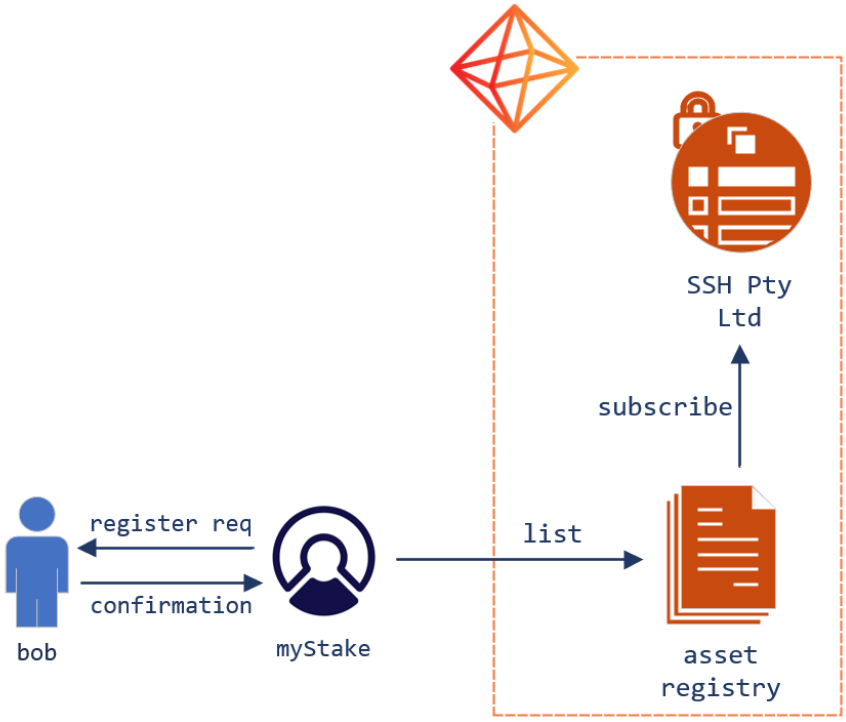


Figure 2: Posting the asset onto an asset catalogue

A.3 Investor Trading

Now that the company has been deployed on the system and on an asset catalogue, any investor can now engage in discovery and purchase of ShellScriptHeavies shares. The discovery process typically occurs via an exchange (provided by another facilitator in the diagram below). The exchange listens for changes to the myStake asset catalogue "Australian Unlisted Company Register", and when it detects that a new company has been added, the user interface is updated with the new information. The ShellScriptHeavies contract has 100 of Bob's shares for sale, offered for settlement in a fixed amount of PET. The offer is configured to settle immediately with no trade time delay. The investor, Alice, views the information and places an order on the exchange to purchase 100 shares (we ignore the process of proof of KYC and accreditation verification for this example). The exchange then submits Alice's transaction to the Programmable Equity Network. The transaction is mined, targets the ShellScriptHeavies registry contract, and executes a trade, updating both Alice and Bob's balance of shares on the ShellScriptHeavies register and balance of PET associated with their accounts. The transaction completes immediately because the contract had been configured to allow all share trades without approval.

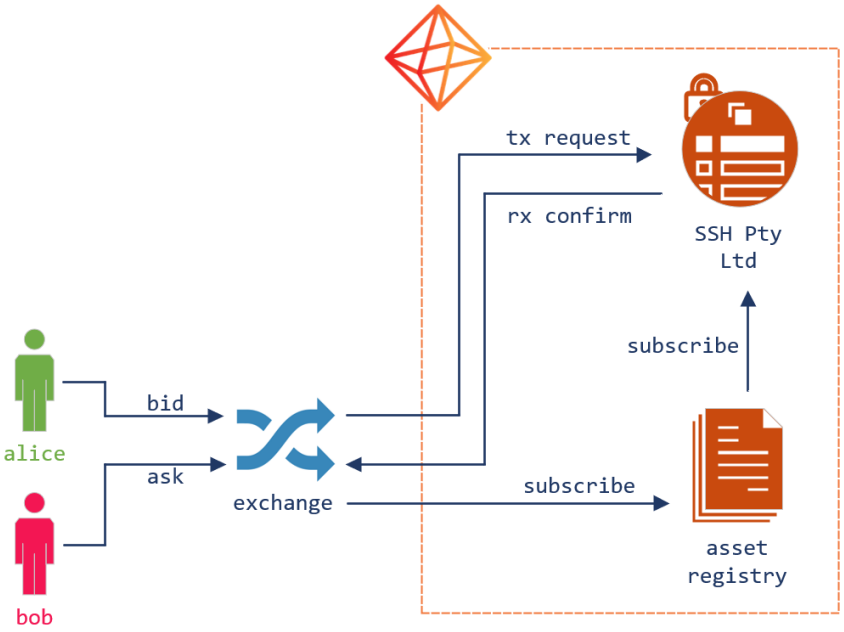


Figure 3: Trading the security

A.3.1 Other Processes

Where settlement is not agreed to be in PET, this can be facilitated by the exchange by providing an escrow service, or simply by mutual agreement between the buyer and seller. myStake, monitoring the contracts, sends a convenient notification to the company secretary (Bob in this case).

On a regular basis, myStake also reminds the ShellScriptHeavies company secretary to update their share registry on ASIC, as there is a requirement to update within 28 days of a trade occurring.

The following diagram provides an overview of some of the high level processes involved in company cataloguing and investor trade:

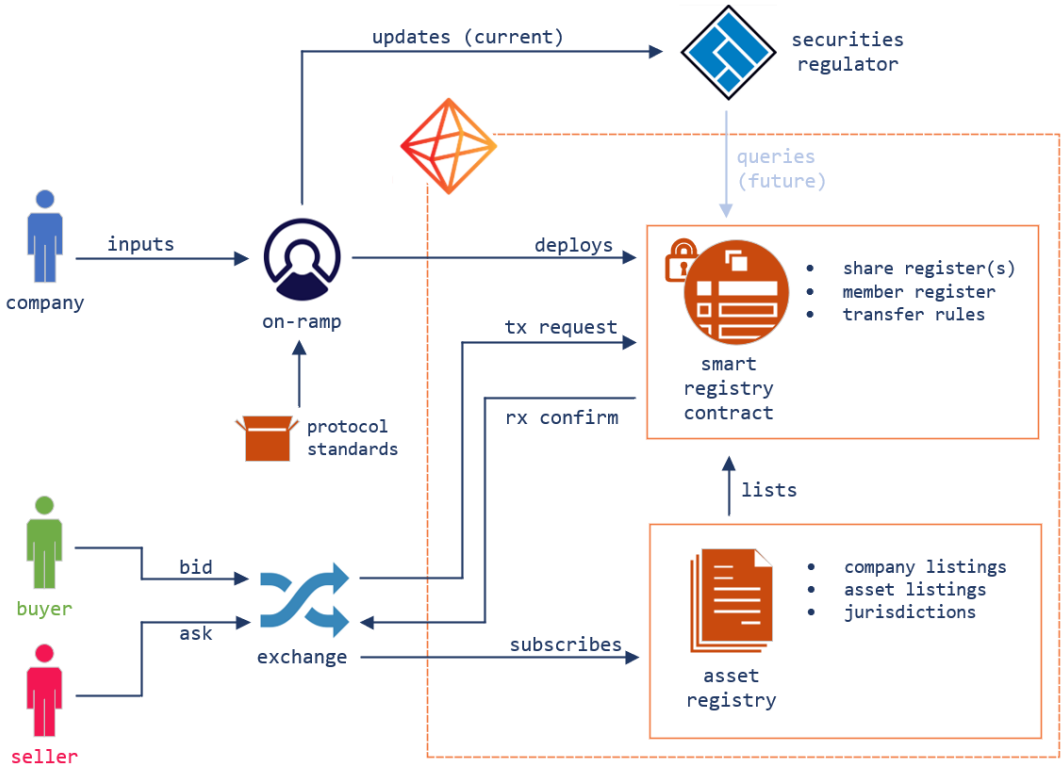


Figure 4: Programmable Equity Network processes

B Draft Standards

B.1 Draft Programmable Equity Protocol Standards (PEPS)

B.1.1 Technical Preliminaries

- Standards can inherit from other standards by the notation Child (Parent). The child contains everything the parent does.
- Mappings can be enumerated to extract the key set; they are specified by `Key -> Value`.
- Collections can in general be deleted cheaply.
- Function definitions are of the form: `name :: functional type signature ? permissions`

B.1.2 PEPS-0: Account

A basic account. All accounts have an owner, which is the person who controls the private key. They additionally have an address space for storing information relevant to that account, such as if they're a director of a company or not.

- Fields
  - `address :: bytes256 (public key of a pair, owner controls the private key)`
  - `balance :: Integer`
  - `store :: Account -> Bytes -> Bytes`
  - `store :: Bytes -> Bytes (Equivalent to store[this])`
- Methods
  - `balance :: Integer (returns PET balance)`
  - `balance :: Register => Integer (calls register.balance(this))`
  - `setStoragePermission :: Account => Boolean => () (grants permission for an account to store info in my profile, by default users can store in their own space)`
  - `updateStore :: Bytes => Bytes => Boolean (stores a given string in user's privileged store at (Sender, String), if permitted)`

B.1.3 PEPS-1: User (Account)

- Fields
  - `name :: String`
  - `mailingAddress :: String`
  - `accreditations/certificates :: Account -> String (mapping from authorities to authorisations for this user)`
  - `contact details :: String -> String`
  - `Other KYC Information :: TBD`
  - `Crypto Keys :: Set(Bytes)`

B.1.4 PEPS-2: Issuer (Account)

A basic generic issuer for tokenising assets.

- Fields
  - `name :: String`
  - `Registers :: Set(Register)`
- Methods
  - `setName :: String => () ? owner`
  - `addRegister :: Register => () ? owner`
  - `removeRegister :: Register => Boolean ? owner`

B.1.5 PEPS-3: Company (Issuer)

All necessary information about a company, its directors, jurisdiction, and so on. Private key no longer privileged: actions can be taken by directors.

- Fields
  - `directors :: Set(Account)`
  - `companyType :: String`
  - `jurisdiction :: String`
  - `identifier (e.g. ACN) :: String`
- Methods
  - `addDirector :: Account => () ? directors`
  - `removeDirector :: Account => Boolean ? directors`
  - `setCompanyType :: String => () ? directors`
  - `setJurisdiction :: String => () ? directors`
  - `setIdentifier :: String => () ? directors`

B.1.6 PEPS-4: Register (Account)

Holds information about who owns what. Shares may not be fractional.

- Fields
  - `issuer :: Issuer`
  - `totalSupply :: Integer`
  - `balance :: Account -> Integer`
- Methods
  - `updateRegister :: Account => Integer => () ? issuer.owner`
  - `transfer :: Account => Integer => Boolean`

B.1.7 PEPS-5: Conditional Transfer (Register)

The general rule under shareholder agreements for most privately owned companies is that shares may not be sold or transferred, except in limited circumstances. This standard allows companies to control the conditions for share transfers. By default, each transfer is manually approved, but if an account is pre-approved, with the permission stored at their own account, for example as a sophisticated investor, transfers can go through instantaneously. The standard also allows for constraining ownership to a limited set of people, and minimum or maximum ownership. The internal logic of the transfer function is left undefined for the purpose of encompassing a broad range of functionality.

- Types
  - `TransferID :: Integer`
- Fields
  - `issuer :: Company`
  - `pendingTransfers :: Set(TransferID)`
- Methods
  - `updateRegister :: Account => Integer => () ? company.directors`
  - `transfer :: Account => Integer => TransferID ? *`
  - `approveTransfer :: TransferID => () ? issuer.directors`
  - `denyTransfer :: TransferID => () ? issuer.directors`
  - `purgeTransfers :: () ? issuer.directors`

B.1.8 PEPS-6: Offers and Settlement (Register)

This standard allows companies to offer shares to their shareholders and third parties

- Types
  - `OfferID :: Integer`
  - `OfferType :: EnumBuy, Sell`
  - `ExpiryDate :: Integer`
  - `Amount :: Decimal`
  - `Price :: Decimal`
  - `Instrument :: String`
  - `Offer :: (OfferId, OfferType, ExpiryDate, Amount, Price, Instrument, Maybe Account)`
  - `Transfer :: (Amount, Price, Instrument, Buyer, Seller)`
- Fields
  - `Offers :: OfferID -> Offer`
  - `Transfers :: List Transfer`
- Methods

- `createOffer :: OfferType => ExpiryDate => Amount => Price => Instrument => Maybe Account => OfferID`
  If offerType is Buy, and the account field is null, it's a generic interest to purchase shares. If the account field is not null, then it is an offer to buy a specific party's shares. The cases for a Sell offerType are similar.
- `acceptOffer :: OfferId => Amount => Boolean`
- `rejectOffer :: OfferId => Boolean ? *`

B.2 Further Standards

The following additional standards will be developed in future iterations of this document:

- PEPS-7 Standard for Pre-emptive rights:
  - Shares must be offered to existing shareholders before offering to 3rd parties
- PEPS-8 Standard for Notifying Shareholders:
  - Notification of offers to shareholders (especially for pre-emptive rights)
  - Notification on transfers
  - Augmented transfer events with settlement information (price, qty, instrument (e.g. AUD vs PET)
  - Notification of document hash
- PEPS-9 Standard for Voting rights:
  - Share class voting weights
  - Codified drag-along clause (Vote to sell company or not)
  - Veto rights for Company Secretary