SEEDSWIPE WHITEPAPER

DIGITAL EQUITY ECOSYSTEM

ARTEMIY MALYSHAU, JEEVAN JUTLA

SeedSwipe is a digital equity ecosystem designed for the internet age. Our protocol enables founders to fundraise seamlessly; from inviting investors, to negotiating terms, and issuing equity all in a single flow. We lower the barrier to equity investment by leveraging our mobile and web platform to enable investors to realize unprecedented liquidity on their investments by making secure investments on chain, trading equity with global peers in a single click.

Contents

1. Introduction

In today's digital age, technology has become a vital part of our daily lives, especially in the world of business and commerce. However, despite this rapid digital transformation, many of the legal systems governing our transactions are still stuck in the past.

Often, the processes behind these transactions are just enough to meet basic requirements, with little thought given to their efficiency or potential for improvement. Many people view them as a mere formality rather than a valuable part of the transaction. This leads to a heavy reliance on legal penalties to enforce trust, lengthy paperwork, and the need for numerous intermediaries. In the world of early-stage private equity investment, these outdated processes can prevent effective collaboration and trap potential value.

This is where smart contracts come into play, offering a revolutionary way to do business. Like traditional contracts, they set the terms of an agreement, but are written in code, enabling them to execute automatically when certain conditions are met, without the need for human intervention. Smart contracts are driven by their internal programming rather than social norms or legal threats, providing a more secure and efficient way to handle transactions.

At SeedSwipe we are leading the charge in transforming outdated business processes into open, digital and decentralized systems, perfect for today's digital world. We've developed the SeedSwipe protocol, a digital equity infrastructure for the backend of our app made up of three main components: SeedShare, SeedClaim and SeedBase. These work together to create a seamless transfer infrastructure for private equity.

In this whitepaper, we're going to detail the SeedSwipe protocol, breaking down its components and showing you how it will change the face of private equity. Section 2 introduces you to the blockchain concepts, like decentralized finance and security tokens. Section 3 details the application and user interface. Sections 4,5 and 6 go into detail about SeedShare, SeedClaim and SeedBase explaining the technology behind them and how they are implemented using Soroban. Finally, section 7 concludes this whitepaper by giving you a clear summary of what we've covered and the potential benefits of the SeedSwipe protocol for private equity.

2. Blockchain Fundamentals

The term "blockchain" was first coined in October 2008 when an anonymous entity under the alias "Satoshi Nakamoto" released a paper describing a new kind of "peer-to-peer electronic cash system." Nakamoto suggested that blockchain could remove the need for trusted middlemen in financial transactions, allowing people to deal with each other directly.

Blockchain works by spreading its data across a large network of computers, which are called "nodes." This is different from traditional security measures that rely on multiple layers of protection and can be very expensive. The blockchain's method is more about spreading out the information so widely that no single part can be easily compromised or attacked.

This setup makes it very hard to tamper with transactions, reducing fears about security for users and offering a transparent system that anyone can join. With blockchain, there's a new kind of digital platform that wasn't widely anticipated before its creation. It's open for everyone to access and built in a way that can be trusted by all who use it.

2.1 Decentralized Finance

Decentralized finance, or "DeFi," is like finance created for the internet age. It's a new, open system that runs on blockchain technology and offers a fresh alternative to the old, often not transparent, and separate ways of traditional finance that have been around for decades.

DeFi covers a wide range of services that deliver on one of blockchain's main promises: enabling financial dealings without the need for traditional middlemen like banks, brokers, trading platforms, or payment processors. These services are available to anyone with an internet connection—you don't even need a bank account or to ask permission from any central figure to use them. Stellar, a prominent player in the blockchain space, is at the forefront of this movement, distinguishing itself through several key initiatives.

Stellar's mission is centered on financial inclusivity, aiming to bring low-cost financial services to underbanked regions of the world. Its platform is designed to be accessible to anyone with an internet connection, removing barriers to entry that many face with conventional financial institutions. This commitment to inclusivity is a core tenet of DeFi and one where Stellar is making significant strides.

The Stellar network is known for its low transaction fees, which are particularly important for users in developing countries and for applications involving microtransactions. By keeping costs minimal, Stellar ensures that its services are affordable for a broader user base, which is essential for the DeFi ethos of universal financial access.

Speed is another area where Stellar shines, with its consensus mechanism enabling rapid transaction settlement. This efficiency is vital for DeFi applications, which often rely on the ability to process transactions quickly and reliably. Stellar's performance in this regard makes it an attractive platform for DeFi developers and users alike.

Even though it's still in the early stages of development, DeFi has the potential to shake up the way we handle money by offering services that are faster, less expensive, and more accessible to more people than traditional centralized financial services.

2.2 Tokens

In DeFi, all transactions happen on the blockchain directly, so traditional money (like dollars or euros) isn't used. Instead, DeFi works with digital assets known as tokens. A token is basically a piece of digital property that can represent ownership. Tokens have different uses; for example, they might stand in for money in a transaction, or they could represent a vote in an online survey. There are mainly two kinds of tokens in DeFi: exchange tokens and utility tokens.

Exchange Tokens
These tokens are designed to be used in a decentralized way, letting owners get goods or services without traditional middlemen like stores or banks. The Financial Conduct Authority (FCA) says that exchange tokens often give holders little or no rights, and there usually isn't a single issuer that holders can demand rights from.

Utility Tokens
Utility tokens let the owner perform certain actions within a specific ecosystem. These tokens can enforce rights within the blockchain by working directly with a system's contracts. The FCA explains that utility tokens give holders access to a product or service that's either available now or will be in the future, but they don't provide the same rights as traditional financial investments.

2.3 Security Tokens

Lately, there's a rising interest in using blockchain technology for turning real assets into digital tokens, especially "security tokens." These tokens are different because they're like digital certificates of ownership for real assets — things like company shares, bonds, or real estate — that have value outside the digital world.

Unlike the more common exchange or utility tokens, which are not regulated, security tokens are more like traditional financial securities. They give the same rights and responsibilities, such as paying dividends or interest. Because of this, they have to follow the same legal rules that apply to regular financial instruments like stocks or bonds. This legal framework means that companies and investors can use them with a lot more trust.

Security tokens are starting to be seen as the next step for financial securities because they promise the reliability of traditional forms with the bonus of being easier to transfer and settle. Even though they're not widely used yet, security tokens are expected to become more popular, driven by the benefits of turning assets into tokens and growing interest from big investors and institutions in blockchain technology.

2.4 Tokenization Benefits

Tokenization offers users a robust platform. Thanks to blockchains secure, open, and tamper-proof record-keeping, security tokens have several benefits over traditional stock exchanges or asset registration systems.

Efficiency
Tokenized asset transactions are completed directly on the blockchain, which cuts out the need for manual processing and significantly speeds up the settlement time.

Cost
The blockchain is built on the public internet, which removes the necessity for private networks for placing orders and complex settlement processes involving many parties.

Security
Blockchain's method of recording and storing data across thousands of computers is more secure than traditional manual record-keeping.

Compliance
With blockchain, regulatory compliance can be integrated at the protocol level, simplifying the management and enforcement of intricate rules, and reducing mistakes.

Transferability
Assets recorded on a public blockchain are more easily transferred, offering a big advantage, especially for assets that are usually hard to sell, like private company shares.

Transparency
Blockchain creates a consistent and independent record that all parties can rely on. This record updates in real-time and is accessible from anywhere, providing clarity for everyone involved.

Composability
Composability means that different assets and blockchain protocols can work together, enhancing each other. This enables the creation of new, innovative financial products that build on and add value to the existing ones.

3. SeedSwipe

SeedSwipe, albeit an infrastructure layer for the time being, will offer an array of frontend applications, ranging from mobile to web, that will enable the creation, management, and trade of the tokenized assets in a manner that is transparent, forward-facing, and clear. This requires careful and thorough considerations for the user experience (UX) for both the consumers aiming to purchase the tokenized assets, as well as the tokenization process to generate those assets to begin with.

The aim of the SeedSwipe frontend is clear — onboard as many consumers as possible, lowering the barriers of entry for consumers that may not be very proficient with web3 jargon or specific terminology and their implications as financial instruments. When translating this aim into a forward-facing product, this means:

1. Following a clear and concise design pattern that encapsulates all the complexities of investing into a tokenized asset while ensuring that the consumer is aware that they are agreeing to a financial commitment.
2. Ensuring that the onboarding process reduces the barrier of entry of entering the SeedSwipe infrastructure ecosystem through an intuitive, but thorough user authentication system. It must be mentioned that financial investments and transactions can only be facilitated once the necessary credentials to conduct this transaction have been entered, this means that the wallet of a user would have to be connected to the app.

3.1 Mobile Frontend

The mobile market size is immense, and thereby offers equally immense potential of capturing a large demographic of users to onboard them not only on to SeedSwipe, but also a wider web3/dApp ecosystem. By making SeedSwipe available as an iOS application, we are opening many users to the potential of investing into tokenized assets. Since Apple has very stringent requirements on the safety and utility of the iOS apps that are uploaded and hosted on their App Store, SeedSwipe will thrive off another added layer of protection, provided natively by Apple. This will contribute to consumer trust, potentially capable of leading a paradigm shift in the widespread impression and opinion of web3 applications.

The purpose of the mobile frontend will be solely focused on the consumers of SeedSwipe, as it will act as a hub for consumers to invest into the tokenized security assets, agree to the conditions of the smart contract, and view their investment portfolio.

3.2 Web-based Frontend

The web-based frontend, in addition to empowering the consumer with investment decisions and a clear and detailed overview, also acts as a platform to onboard companies and partners to tokenize their assets. The process of onboarding companies and partners obviously requires several verification steps to perform the due diligence that is necessary to ensure that the stringent and strict process is performed thoroughly and correctly.

This means that, the web-frontend will provide an easy-to-use, concise, and clear frontend, similarly to its mobile counterpart, while ensuring that potential partners and companies have an accessible avenue to express their interest in joining the wider SeedSwipe ecosystem by permitting the tokenization of their assets.

4. SeedShare

SeedShare is a tool based on Soroban smart contracts, designed to streamline the process of managing and handling tokenized equity. It enables users to issue, transfer, manage and hold tokenized shares, set up compliance rules and automate the administration of share registers. By leveraging automation and blockchain's inherent trustlessness, SeedShare simplifies interactions between parities eliminating the need for intermediaries.

We've taken a unique approach with SeedShare, choosing to distinguish equity tokenization from Equity Token Offerings (ETO's). Although these concepts are closely linked, they are not dependent on each other, ETO's which involve public crowdsales, require tokenization of equity but once tokenized it doesn't have to be distributed through a public sale, in fact, for most users, ETOs are not necessary and can introduce complex and legal regulatory challenges.

While equity crowdfunding campaigns are often seen as a straightforward alternative funding method, they come with their own set of challenges. By removing ETOs from our core product, we've made issuing digital equity a much simpler process, requiring minimal change or commitment from users. SeedShare is initially targeting private, primary market transactions between issuers and validated investors allowing benefits to be realized in as little as half an hour compared to the months it might take for an ETO.

We believe that equity tokenization has not yet reached its full potential, despite its clear advantages over current tools and practices. Token issuance still depends on various actors like advisors, law firms and custody agents. What makes SeedShare's value offering so compelling is that it's simple. Instead of manually sharing legal agreements in PDF form, signing them physically or with tools like DocuSign, manually updating the shareholder register and issuing share certificates, SeedShare provides a single integrated process for both issuers and investment professionals to streamline their legal, administrative and transactions activities.

Unlike traditional equity management tools such as Carta, which uses a disconnected private database, SeedShare utilizes the blockchain to maintain a synchronized, open record of ownership. This ensures that ownership information is secure and accessible to this with the right permissions, whether they are shareholders making transfers or third-party applications. Users have full control over their assets, while also benefiting from a transfer infrastructure that can be built upon and integrated with by third parties.

Open, standardized protocols have played a crucial role in the development of major platforms like the web. By creating a shared standard for representing equity on the blockchain, we aim to foster collaboration and participation in ways previously unimaginable. Just as a currency gains value from being widely accepted, the broader recognition of digital equity assets increases their value. From instant equity-backed loans to secondary markets, the blockchain opens a myriad of exciting possibilities. With a process that can take as little as half an hour, we believe this is an exceptionally straightforward way for issuers to enhance the value of an asset and make an investment opportunity more appealing.

4.1 Equity Tokenization

The basic process for equity tokenisation is as follows:

1. **Structuring**
   Configure the basic details of the asset by defining its name, ticker, supply and more. Structure the asset type and build the legal agreement from a library of modules or upload your own legal agreement to be encoded.

2. **Compliance**
   Define the compliance rules for the asset. This includes transfer holder location, holder verification and KYC, total holder limits, non-fractionality, non-transferability and more. Any whitelisted addresses are exempt otherwise compliance rules are enforced at the protocol level.

3. **Creation**
   Key information is encoded in a digital format. A hashed bidirectional link is created; a bidirectional link is created between the token and the legal agreement proving they have not been tampered with. The token is deployed on Stellar. Legal agreements are uploaded and deployed to IPFS.

4. **Issuance**
   Create shares and invite investors to receive them via a private link. Investors can create an account in a few simple clicks, review and cryptographically sign digital legal agreements and receive their shares.

5. **Management**
   The shareholder register is automatically rendered and updated. This on-chain record may serve as the definite record of a company's shareholders or can be explored to an offline shareholder register. If issuers need to act, they have a suite of tools such as share recovery, force transfer and freezing.

4.2 Regulator Requirements

One of the most important attributes of equity tokens, as compared to utility or exchange tokens, is that they are subject to existing securities laws. Any design for equity tokens must remain compliant with legal and statutory requirements. Furthermore, such a solution should provide issuers with several fine-grain controls.

The 8 key attributes for equity tokens are:

1. Be upgraded without changing the token smart contract address.
2. Implement multiple tokens in a single smart contract.
3. Embed legal agreements in a way that is secure and legally binding.
4. Apply any rule of compliance that is required by the token issuer or regulator.
5. Have a standard interface to pre-check if a transfer is going to pass or fail.
6. Provide an up-to-date list of token holders.
7. Have a recovery system in case an investor loses access to their account.
8. Be able to freeze a token in a shareholder's wallet partially or fully.

4.3 Multitoken

SeedShare is designed to facilitate the issuance of equity in a manner that is secure, compliant, and effortlessly smooth for users. The ERC-20 standard, initially created for standalone assets, demands the repetitive deployment of identical contract frameworks for each new asset, which introduces inefficiencies, extensive resource use and elevated risks. This approach is particularly problematic for specific applications such as alphabet shares.

SeedShare differentiates itself by using the ERC-1155 multi-token standard at its core, in contrast to other permissioned tokens. This advanced standard enables the simultaneous implementation of an unlimited number of tokens under a single smart contract. The creation of a new token adds a unique identifier to the existing list within the contract, complementing the unique contract addresses found in ERC-20 token implementations. Consequently, SeedShare introduces an 'id' function argument serving as a distinct identifier for each token. Despite the shared contract across multiple tokens their accounting operator control and compliance controls remain meticulously separated, distinguished by the token ID.

4.4 Compliance Control

SeedShare stands out with its distinctive approach to ensuring compliance directly at the protocol level. In contrast to the ERC-20 standard, where token transfers typically fail only due to insufficient funds on the part of the user. SeedSwipe introduces a broader range of potential failure points to enhance compliance and security. These include scenarios where the recipient has not completed necessary KYC verifications, instances where assets are locked or frozen, as well as various economic and jurisdictional restrictions, such as limits on shareholders, acquisitions, and geographic considerations.

Paradoxically we believe that implementing stringent transfer controls paves the way for increased asset transferability. Without these robust mechanisms in place, regulators are unlikely to authorize the widespread tokenization of regulated assets. Additionally, issuers would be hesitant to support automatic on-chain resolution of asset transfers. By proactively addressing these challenges at the protocol level, SeedShare ensures a smoother, more secure, and compliant process for all parties involved.

4.5 Advanced Issuer Controls

SeedShare includes several advanced issuer controls designed to facilitate effective and secure equity tokenization, including:

- pause/unpause
- recover
- unfreezePartialShares/freezePartialShares
- batchFreezePartialShares/batchUnfreezePartialShares
- setAddressFrozen
- batchSetAddressFrozen

4.6 Compliance Suite

The SeedShare token operates in conjunction with an on-chain validator system, meticulously recording and enforcing compliance controls for every transaction to confirm the eligibility of both the transfer and the recipient. This compliance suite is versatile, enabling the definition and enforcement of a broad spectrum of crucial parameters. It offers an open, programmable method to automate compliance, effectively shifting a substantial portion of the responsibility from operators to the protocol itself. Initially, SeedSwipe is concentrating on establishing a set of rules and transfer controls with universal applicability, with plans to augment the compliance contracts with more detailed rules tailored to specific jurisdictional requirements as the protocol evolves.

SeedSwipeCompliance
The SeedSwipeCompliance contract streamlines the verification processes by automating the validation of recipient account properties. Working in tandem with the SeedClaimRegistry (see section 6 for details), it ensures that the receiver is either whitelisted and thus exempted or possesses the necessary credentials to acquire equity tokens. This contract scrutinizes the properties of the interacting entities, enforcing the defined parameters and returning a true or false outcome based on the transfer's eligibility status.

SeedSwipeRegistry
The SeedSwipeRegistry contract plays a pivotal role in documenting ownership, applying token-based transfer limits (such as verifying transfers are non-fractional, confirming holder count or specific jurisdictional limits are within acceptable bounds) and imposing holder-based transfer restrictions (ensuring for example that transfers are not originating from a frozen address or using frozen tokens). This registry offers substantial advantages over traditional manual register administration practices, significantly diminishing inefficiency, overheads, and inaccuracies. This results in providing companies with a more efficient platform to meet statutory obligations. Additionally, as the share register is capable of interfacing with external machine systems, there is potential to further streamline the process through automatic filings.

4.7 Legal Smart Contracts

Legal and regulatory considerations have significantly influenced the development of the SeedSwipe protocol. It's important to acknowledge that smart contracts are not universally applicable or suitable for all types of situations. Especially when it comes to interactions involving humans or off chain activities, traditional legal agreements remain the most effective way to formalize these agreements.

SeedSwipe goes beyond just offering on-chain solutions; it facilitates the creation of smart legal contracts. These contracts blend automated and traditional elements allowing certain obligations to be tracked, enforced, and executed automatically through smart contracts, while others are documented in plain text and upheld using conventional legal procedures.

To put it simply, SeedSwipe transforms legal agreements into a format that is readable by machines. These agreements maintain the legal enforceability and can be signed using cryptographic methods. They can also be interpreted by

external machine systems, allowing for search, analysis, and integration by third-party entities.

This approach doesn't just create a robust legal foundation for users, ensuring that SeedSwipe equity is treated as a legitimate digital asset (as opposed to just a tokenized representation of an off-chain asset). It also sets the stage for unprecedented levels of automation by making information accessible and interpretable by machines.

Structure

Metadata: records the key terms contained within the agreement in a machine-readable format.

Markdown: records and captures the terms of the legal agreement in a human-readable format

Smart Contracts: Enforce the relevant terms from the agreement on-chain.

4.8 Metadata

SeedSwipe introduces a metadata model designed to make the essential terms of an agreement easily accessible and interpretable by machines. This approach significantly improves the compatibility and functionality of third-party applications, as it extracts and organizes crucial information from the agreement. Consequently, external machine systems can index and use this information efficiently.


```
{
        "name": "Acse Ordinary Shares",
        "symbol": "ACSE",
        "description": "Asce limited fully paid ordinary shares",
        "image": "ipfs:./QmW78TSUVA2343HCADk..../acselogo.png",
        "agreement": "ipfs:./QmWS1VAdMD353A6SDk..../agreement.md"
        "agreementMetadata": {
                "$class":
                "org.seedswipe.tokenHolderAgreement.tokenHolderClause",
                "companyName": "ASCE LIMITED",
                "companyNumber": "123456789",
                "companyIdentity": "acse.seedswipe",
                "acceptedCountries": ["United Kingdom", "France", "Germany",
                "Sweden"], "signatureRequired": "True", "asset": { "$class":
                "org.seedswipe.assets.ordinaryShare",
                "shareFullyPaid": "True",
                "shareFractional": "False",
                "shareTransferLimit": "False",
                "shareHolderLimit": "False",
                "clauseId": "N234JKHKNM-8791-2146-AD7Y-8YRjgK24121L4K "
                },
        "clauseId": "45KNKL43NL-8932-5434-231n-083kjn21kjn3w"
        }
}
```

Encoding
In the creation and encoding of smart legal contracts, SeedSwipe establishes a secure connection between various elements. It achieves this by forming a two-way link, effectively mapping out the intended relationship between the legal contract and its smart contract counterpart, noted in the token URI. This method ensures a cryptographically secure integration, providing a safeguard that guarantees the integrity of information recorded off-chain, making it resistant to tampering.

An example of a token holders' agreement, the steps are:

1. The user inputs data via the application.
2. This data is then used to create a structured metadata model using JSON.
3. A new token is created in the SeedShare token contract with a unique identifier.
4. The metadata model is updated with the terms of the agreement to be enforced on-chain from the structured data model, referencing the token identifier.
5. The compliance contract is updated with the terms of the agreement to be enforced on-chain from the structured data model, referencing the token identifier.
6. The metadata is used to render the legal agreement in Markdown.
7. The legal Markdown file is uploaded to IPFS.
8. The metadata is updated with the legal agreement IPFS URI.
9. The metadata JSON file is uploaded to IPFS.
10. The SeedShare token is updated with the structured metadata model IPFS URI.

5. SeedClaim

SeedClaim is the decentralized platform focused on credentialing, aiming to assist the SeedSwipe community in establishing and onboarding a list of reliable verifiers for credentialing services. It enables users to create digital identities though claims, which are digitally signed statements confirming specific attributes of an account. These identities play a crucial role in compliance procedures that depend on credentials.

The intersection of regulated assets and decentralized, permissionless protocols introduces a complex set of technical, ethical, and regulatory challenges. Blockchain has successfully eliminated intermediaries in financial transactions, directly connecting buyers and sellers. This advancement has led to a more efficient and equitable system but also resulted in a significant reduction in regulation. Consequently, the decentralized finance space has experienced frequent occurrences of security breaches and deceptive practices.

Regulatory bodies have been striving to adapt to the rapid changes within the blockchain ecosystem, but their efforts have largely been ineffective. They often resort to a conservative approach and strict regulatory measures to safeguard users. However, this reactive strategy has proven to be insufficient, primarily because it doesn't address the underlying issues that have historically affected financial markets and that blockchain technology aims to resolve. High-profile controversies involving regulated entities, such as Celsius and FTX, highlight that regulatory approval and oversight alone cannot ensure user safety.

Rather than reverting to centralized methods or downplaying the importance of trust we advocate for a balanced approach. This involves recognizing and incorporating traditional and legal regulatory controls in a manner that aligns with the principles of web3. Our goal is to foster trust in operations that can't be automated or executed on-chain, white simultaneously preserving the decentralization, trustlessness and privacy inherent to blockchain technology as much as possible.

5.1 Digital Identities

Digital identities are crucial for safe and regulated online interactions, especially when using the SeedSwipe protocols. They help users, trust each other when interacting online, create legal agreements that are binding and use smart contracts to automatically check credentials and ensure compliance. This creates a trustworthy digital environment, which makes it easier to complaint parties to participate and reduces obstacles.

5.2 Claims

A blockchain account on its own doesn't hold any value. To truly understand the person or group behind the account, you need 'claims.' Claims are like digital notes, signed with cryptography, that say the account has certain characteristics or features. These can be confirmed by the user themselves, other users, or a trusted third-party credentialing system. Claims make it possible to quickly verify information, letting smart contracts immediately check and validate user attributes directly on the blockchain.

With claims we can automate and enforce transfer controls and compliance right at the protocol level. As an account collects more claims, a usable model of identity starts to form. In the past, someone had to manually check who could become a shareholder. Now with claims issuers can set specific characteristics that need to be met before someone can receive shares. This automation makes it much easier to move shares around, which we believe will make private equity investments more liquid and easier to trade.

We see claims playing a big role in the SeedSwipe ecosystem, becoming even more important as it grows. SeedSwipe's goal is to create a worldwide compliant chain system for private equity investments. However due to the complexity and differences in regulations around the world, claims will initially be used mainly to check statements in interactions related to credentials.

Claim Verification
An example of the verification process for a credential-based interaction is:

1. AcseKYC creates a SeedSwipe account.
2. SeedSwipe verifies AcseKYC as a trusted verifier for KYC.
3. To participate in one of any number of investment opportunities a prospective investor may need to verify that they are identify verified or an accredited investor on the platform.

5.3 Trusted Verifiers

SeedSwipe aims to offer a neutral platform, serving as the foundation for a network of 'trusted verifiers.' These verifiers are reliable third parties that carry out credentialing services within the SeedSwipe ecosystem. In return for economic rewards, verifiers can provide claims, confirming the validity of specific information. When a claim is issued by a trusted verifier others can trust its accuracy without needing to check it themselves.

It's crucial to note that to keep its decentralized nature and maintain its role as an infrastructure platform, SeedSwipe won't control or decide who becomes a trusted verifier. Instead, the community of SeedSwipe users will manage and oversee the list of trusted verifiers using the SeedBaseVerifiersCurator contract.

This contract essentially functions as a token curated registry (TCR), striving to create a fairer and more balanced curation process than typical regulatory approvals. The registry operates based on a set of rules, determining which items can be included on the list. These rules are upheld through a voting system, where token holders get to voice their opinions on adding or removing items from the registry. This approach fosters a self-governing marketplace, where the community of token holders influences both the token's value and the quality of the items listed in the registry.

6. SeedBase

SeedBase is a secure and user-friendly smart contract account designed to be light and efficient. It simplifies the user experience by eliminating the need for private key management while keeping the system fully decentralized. High-risk actions are protected with easy-to-use multi-factor authentication, requiring either multiple devices or team members to give their approval.

Today's blockchain technology is like the early days of the internet: the technical foundation is strong and ready for widespread use, but there are still significant useability issues that make it difficult for non-technical users to adopt. Most blockchain applications today are created 'by developers for developers' with little consideration on the average user.

Many blockchain enthusiasts strongly support the idea of self-custody but it's important to understand that simplicity is often more important for the average user than having control. For blockchain applications to truly become mainstream, the technical details need to be hidden from the user, making the system easy to use. Understanding blockchain should be an option for those interested, not a requirement for participation.

Currently, blockchain accounts are easily created and discarded, which has led to a lack of meaningful user experiences and support for registered assets. Privacy is important, but the disposable nature of blockchain accounts has held back progress in the space.

Our solution is SeedBase, a lightweight multi-factor smart contract account that significantly improves the user experience by removing the most risky and complicated aspects. Importantly, SeedBase achieves this whole preserving all the benefits of decentralization ensuring that assets remain securely in the hands of the owners.

6.1 Smart Contract Account

At the heart of SeedBase is a smart contract wallet, working as a proxy account contract that lets users carry out transactions. This account is linked to a key-value store, holding numerous keys any of which can initiate a transaction.

Multisignature
To go ahead with a transaction, the account needs approval from at least one additional key. This multi-signature requirement lowers the risk of single-point failures and adds an extra layer of security for high-risk transactions. Users have the flexibility to set the number of required approvals depending on the type of transaction.

Subdomain Identifiers
Users expect accounts to have easy-to-remember identifiers like names, username, or email addresses. Instead of a lengthy 42-character public key, SeedBase assigns accounts and objects unique subdomain identifiers, creating a user-friendly and clear way for interactions.

Local Keys
To balance ease of access and security while ensuring users maintain direct control of their assets, SeedSwipe employs numerous disposables, context-specific key pairs. These function as standard externally owned account (EOA) wallets but are used solely to sign transactions locally, meaning they never hold any funds. Funds are kept in the user's main identity account. When accessing their identity account from a new user, create a new key pair stored locally on that device. They then request permission to add this new key to their account, which existing keys must approve. Once approved, the new key is added to the account.

Meta Transactions
One major hurdle for adopting blockchain applications is the need to pay network fees, or 'gas' for transactions. Users must buy network tokens or hold multiple tokens for a single transaction, creating a barrier to entry. Meta transactions, also known as relays, offer a solution by allowing a third-party relayer to execute transactions, effectively bypassing direct network fee payment. While network tokens are still needed to complete a transaction, and thus meta transactions are not technically 'gasless' they do enable a third party to cover the cost. SeedBase utilizes this relay method allowing gas fees for all covered transactions to be externally handled by its revenue model.

To execute a transaction from a SeedBase user account:

1. A request is generated in the browser for a transaction the user would like to execute.
2. The transaction request is signed with their local private key.
3. The transaction request is sent to the SeedSwipe relay.
4. The relay wraps the transaction request within another transaction, the meta transaction and submits the transaction to the identity account contract.
5. The identity account contract unwraps the meta-transaction and executes the transaction the user has requested.

Account Access
To access a user account the user inputs a personal account subdomain such as "monkey.man.seedswipe".

If the user has an account and key:

- The local key is used to sign and send the transaction via relay.

If the user has an account but no key:

- A new local key is generated and stored on the device.
- The local key is added as a new signed to a relay transaction.
- This transaction is then confirmed and set from a key with the appropriate permissions. For example, a user may sign the transaction by adding their smartphone from their laptop.

If the user does not have an account:

- A new local key is generated and stored on the device.
- A new SeedBase account is deployed to the blockchain via relay, with the local key added as having top-level privileges.
- The user selected subdomain is registered to the user's account address.

7. Conclusion

The SeedSwipe protocol is designed as a flexible framework for turning company shares into digital tokens. The familiar mobile and web UI is built to be easy for anyone to join and is dedicated to maintaining the core ideas of Stellar and web3, openness and decentralization, even as it deals with assets that are under regulatory scrutiny. This dual focus aims to strike a balance between the control regulation offers and the freedom of decentralization.

SeedSwipe 1.0 doesn't directly support regulated actions like verifying credentials (KYC), investing, or raising money for companies. It provides an open, standardized service for this to be built on later.

The vision for SeedSwipe is more than just a tool for managing digital shares. It's about setting up a comprehensive digital system for handling equity. It could enable secure online shareholder voting, create marketplaces for buying and selling these digital shares, provide instant loans backed by equity and help set up companies directly on the blockchain. These are just a few possibilities that could greatly improve how flexible, accessible, and profitable start-ups and venture capital ventures are on a global scale.

SeedSwipe's unique approach lies in its unbiased platform for digital share management, contracting with isolated, in-house databases or traditional, highly intermediated tokenization services offered by broker-dealers. By creating a layer for transferring and owning equity that fits well with the global start-up and venture capital world, SeedSwipe stands out with its potential to revolutionize how we handle company ownership and investment.