HYPERSURFACE: A DIGITAL EQUITY INFRASTRUCTURE PROTOCOL

1. Introduction

In the 21st century, digital systems cut across every aspect of organisational and commercial relationships. Computers and the internet have quickly become central to our modern world. Yet, from a historical perspective, they are still in their infancy. While our society has become increasingly digital and distributed, the legal controls that coordinate the execution of society's transactions have not followed the same trajectory.

Beyond meeting the minimum requirements, often, no real thought is given to how these processes are structured. The general feeling is that as long as they're good enough the way they're implemented doesn't particularly matter; that they're more of a formality, rather than a driver of value. As a result, trust is assured through the threat of legal penalties, even the simplest procedures can require voluminous paperwork and operations are dependent on a litany of intermediaries and counterparties. In early-stage private equity investment, poor asset transferability is just one example of how these disconnected analogue processes hinder collaboration and silo value.

As "software eats the world", powerful, non-legal mechanisms to regulate interactions have begun to emerge. Smart contracts offer a radical new paradigm for business. Like a traditional legal contract, a smart contract establishes the terms of an agreement. Unlike a traditional agreement, however, a smart contract's terms are rendered and executed as code.

Whereas the burden of upholding a legal agreement falls solely on its participants, a smart contract will automatically self-execute upon the fulfilment of certain predetermined conditions, irrespective of human involvement. Smart contracts are compelled to act in a certain way, not by social norms or by the threat of punishment, but by their hardwired internal logic, by their architecture. By transcribing the legal and contractual provisions that reside at the heart of a company to a blockchain environment, many of the procedures that make up a business can be rendered and executed automatically.

Hypersurface is reinventing the systems that underpin modern enterprise. Our aim is to transform the static, disconnected processes we are familiar with today into ones that are open, digital and decentralised. We envision a new era of technologically-mediated hybrid organisations, designed for the age of the internet.

As the first step toward such an ecosystem, we have developed the Hypersurface protocol, a digital equity infrastructure consisting of three key elements: Hypershare, Hyperclaim and Hyperbase. These three components work together to create an open, general-purpose transfer infrastructure for private equity.

In this paper, we outline the nature and value of the Hypersurface protocol. Section 2 provides an introduction to some existing concepts from the blockchain, such as decentralised finance and security tokens. Sections 3, 4, and 5, introduce the protocol components, Hypershare, Hyperclaim and Hyperbase respectively, providing an overview and details regarding the technology and its implementation. Section 6 provides a conclusion.

2. Existing Concepts

The term “blockchain” was first coined in a white paper published in October 2008, by an anonymous person or group of people known as “Satoshi Nakamoto”. The paper detailed a “peer-to-peer electronic cash system”. Nakamoto’s vision was to use the blockchain to bypass the need for trusted third parties, allowing people to transact directly with one another.

To do so, the blockchain makes use of a system state that is distributed across a network of computers or “nodes”. Whereas security in centralised infrastructure is created through a “defence-in-depth” approach, often relying on tens of millions of dollars of technical resources and many layers of security, in many ways, the blockchain can be considered “defence-in-breadth”. By spreading the system state across a network of nodes, no single point is vulnerable to coercion or attack.

This design makes it extremely difficult to falsify transactions, meaning user uncertainty regarding security is minimised while creating a completely public system that anyone can use. In this regard, the blockchain satisfies a need that few people recognised before its advent: that of an independent digital execution platform. One that is open and accessible to the public, and can be trusted by all participants.

2.1. Decentralised Finance

Decentralised finance (“DeFi”) is finance for the age of the internet, an open global system running atop the blockchain, offering the first radical alternative to the disconnected, opaque, decades-old practices and infrastructure of traditional finance. DeFi encompasses a vast array of services that fulfil one of the blockchain's core possibilities: fostering financial transactions that aren’t officiated by banks, brokers, trading platforms, payment processors or any other type of intermediary. These services can be used by anyone with an internet connection, without the need for a bank account or permission from a central authority. Although still in its early stages, DeFi has the potential to disrupt the traditional financial system by providing faster, cheaper and more accessible financial services than its centralised counterparts.

2.2. Tokens

In DeFi, transactions are settled directly on the blockchain. As a result, they don’t allow for the use of fiat currency. Instead, they deal exclusively with crypto assets such as tokens. A token is a blockchain-native digital asset that typically represents a unit of ownership. Tokens can be used in a variety of ways. For example,

a token may be used to represent a certain amount of currency in a financial transaction, or, alternatively, a token could be used to represent a vote in an online poll. Tokens typically belong to one of two categories: exchange and utility tokens.

Exchange tokens

Exchange tokens are intended as a decentralised tool that allows holders to access goods and services without the use of traditional intermediaries. The FCA states that “[exchange] tokens are designed to provide limited or no rights for token holders, and there is usually not a single issuer to enforce rights against”.

Utility tokens

Utility tokens grant the bearer the ability to perform certain actions within a specific ecosystem. These tokens often enforce rights on-chain by interfacing directly with a protocol's contracts. The FCA goes on to state that “[utility] tokens grant holders access to a current or prospective product or service but do not grant holders rights that are the same as those granted by specified investments”.

2.3. Security Tokens

In recent years, there has been a growing interest in the use of blockchain for asset tokenisation. In particular, for “security tokens”. A security token is a unit of ownership recorded on the blockchain. Security tokens are distinct from unregulated tokens, such as exchange and utility tokens, in that they often represent real-world assets (“RWAs”) with value external to the blockchain, such as shares, bonds, and property.

Security tokens are typically classified based on whether they provide the same rights and obligations as traditional securities, and regulated based on their shared substantive properties. For security tokens to be recognised and issued as such to investors, they must meet the same requirements specified under applicable securities law for similar fiat instruments. As security tokens sit within established regulatory frameworks, traditional issuers and investors can engage with much greater confidence.

Security tokens are increasingly seen as an inevitable evolution of mainstream securities, as they provide many of the assurances and controls of traditional securities but with enhanced transferability and settlement. Although security tokens have not yet seen large-scale adoption, they are likely to grow in the coming years. This growth will be driven by the significant advantages offered by tokenisation, as well as increasing institutional interest in the underlying technology.

2.4. Tokenisation Benefits

Tokenisation provides a powerful platform for users. With the blockchain providing a secure, transparent and tamperproof means of record-keeping, security tokens present a number of advantages over traditional stock exchanges or asset registries.

Efficiency

Transactions for tokenised assets are settled directly on the blockchain, bypassing the need for manual administration procedures and dramatically reducing settlement time.

Cost

Blockchain technology is built atop public internet infrastructure eliminating the need for private order routing networks and complex, highly-intermediated settlement procedures.

Security

Blockchain technology is more secure than traditional forms of manual record keeping as the system state is recorded and stored across thousands of computers.

Compliance

Blockchain technology enables compliance to be implemented directly at the protocol level, making it easier and less error-prone to manage and enforce complex procedures.

Transferability

With assets encoded on a public blockchain network and transfers assured by non-legal mechanisms, token holders benefit from significantly increased asset transferability. This is particularly significant for illiquid assets such as private equity.

Transparency

blockchain technology creates a single record of truth that is independent and all parties can trust. This synchronised state is updated automatically and can be accessed from anywhere.

Composability

Composability allows entire ecosystems of assets and blockchain protocols to work together synergistically. This means innovative new product offerings can be built atop existing ones, leveraging the resources made available by its predecessors and in turn, adding value to them.

3. Hypershare

Hypershare is a set of smart contracts for equity tokenisation that allow users to issue, transfer, hold and manage tokenised equity, program compliance rules and automate share register administration. Hypershare harnesses automation and trustlessness to structure interactions between parties, without the need for intermediaries.

Unlike contemporary tokenisation platforms, for Hypershare we have chosen to separate the notion of equity tokenisation from equity token offerings (“ETOs”). While the concepts of equity tokens and equity token sales are highly interrelated, they are not mutually interdependent. Whereas ETOs rely on tokenisation of the underlying asset, equity, once tokenised, does not demand a public crowdsale as its primary distribution method. ETOs are neither necessary nor appropriate for the majority of users and introduce significant regulatory and legal considerations.

Like equity crowdfunding campaigns, what is often perceived as a simple, effective form of alternative funding comes with its own set of drawbacks and considerations. By removing ETOs from the core product offering, issuing digital equity requires very little behavioural change or commitment on the part of users. For its initial release Hypershare targets private, primary market transactions between issuers and accredited investors. Whereas an ETO could take several months from end-to-end, without the regulatory and legal concerns that accompany large public crowd sales issuers may start to see benefits in as little as half an hour.

In our view, there has not been a single product or service that has realised the full potential of equity tokenisation. Equity tokenisation offers significant benefits compared to contemporary tools and practices. However, it is by no means a simple process. Token issuance is still dependent on an array of actors such as advisors, law firms, broker-dealers, KYC/AML providers, custody agents, cap table management solutions, and more. Part of what makes Hypershare’s value offering so compelling is that it is 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, Hypershare provides a single, integrated process for both issuers and investment professionals to streamline their legal, administrative, and transactional activities.

The key distinction between Hypersurface and current equity management tools, such as Carta, is that rather than using a disconnected private database, Hypersurface makes use of the blockchain to create a synchronised, open record of ownership. With ownership and transactions secured by the blockchain, information is rendered and available to read and write by anyone with appropriate permissions. This could be a shareholder

transferring shares or a third-party application. This gives users complete ownership over their assets while simultaneously creating a composable transfer infrastructure that can be integrated and built on top of by third parties.

Open, standardised protocols have been instrumental in the development of many platforms such as the web. By creating a shared standard for representing equity on the blockchain, our aim is to enable people and organisations to participate and collaborate in ways that would never have before been possible. In the same way that a currency is only valuable in that it is a widely recognised means of exchange, the more broadly digital equity assets are recognised the more valuable we believe they will become. From instant equity-backed loans to secondary markets, the blockchain opens up a whole host of new and exciting use cases. For a process that could take as little as half an hour, we see this as potentially the easiest way for an issuer to increase the value of an asset and the appeal of an investment opportunity.

3.1. Equity Tokenisation

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 and edit 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 between the token and the legal agreement proving they have not been tampered with. The token is deployed on the blockchain. Legal agreements are uploaded 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 definitive record of a company's shareholders or can be exported to an offline shareholder register. If issuers need to take action they have a suite of tools such as share recovery, forced transfers and freezing.

3.2. Regulatory 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.

We identify eight key attributes for equity tokens:

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 tokens in a shareholder's wallet, partially or fully.

3.3. Multi-token

The goal of Hypershare is to enable the issuance of equity in a way that is secure, compliant, and frictionless for users. As the ERC-20 standard was developed for standalone assets, any ERC-20-derived security token would require multiple deployments of the same contract for each new asset with little to no change between implementations. Needless to say, this is inefficient, resource-intensive, and risky, particularly for use cases such as alphabet shares.

Unlike other permissioned tokens, at its core Hypershare uses the ERC-1155 multi-token standard. The ERC-1155 uses a single

smart contract to implement an arbitrary amount of tokens at once. When a new token is “created” a unique identifier is added to the list of tokens contained within the contract. This identifier supplements the unique contract address associated with ERC-20 token implementations. Accordingly, Hypersurface features an additional “id” function argument that serves as the unique identifier for each token. Although the contract is shared amongst multiple tokens, the accounting, operator controls and compliance controls are partitioned based on the token id.

3.4. Compliance Controls

A unique feature of Hypershare is that it enforces compliance at the protocol level. Unlike the ERC-20, where token transfers only fail due to the user having inadequate funds, Hypershare transactions can fail for a variety of reasons. These include the receiver not having verified KYC information, assets having been locked or frozen, and economic and jurisdictional constraints such as shareholder, acquisition, and geographic limits.

Somewhat counterintuitively, we believe that stronger transfer controls will increase asset transferability as without them (a) regulators will not permit large-scale tokenisation of regulated assets and (b) issuers will not support automatic on-chain transfer resolution.

3.5. Advanced Issuer Controls

Hypershare features several advanced issuer controls designed to facilitate effective and secure equity tokenisation, including

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

3.6. Compliance Suite

The Hypershare token is coupled with an on-chain validator system that records and enforces compliance controls on every transfer, ensuring that the transfer and recipient are eligible. The compliance suite can be used to define and enforce a wide range of key parameters and provide an open, programmable means of automating compliance, shifting much of the burden away from operators and onto the protocol itself. For its initial release, Hypersurface is targeting a set of rules and transfer controls that are universally applicable. As the protocol grows, we hope to add

further detail to the compliance contracts, implementing new rules in accordance with specific jurisdictional requirements.

HypershareCompliance

Instead of manually checking each interaction, the HypershareCompliance contract can be used to define and verify the essential properties of a recipient account. In combination with the HyperclaimRegistry (see Hyperclaim), the HypershareCompliance contract verifies that the receiver is either whitelisted and therefore exempt, or that the receiver has the appropriate credentials to receive equity tokens. The compliance contracts then read the properties of the interacting identities to enforce these specified parameters, either returning true or false based on the eligibility status of the transfer.

HypershareRegistry

The HypershareRegistry contract (1) records ownership, (2) enforces token-based transfer limits, such as ensuring a transfer is non-fractional, the maximum holder count or specific jurisdictional limits have not been exceeded and (3) enforces holder-based transfer restrictions, such as ensuring that transfers are not being made from a frozen address or using tokens that are frozen. The HypershareRegistry provides significant benefits over current manual register administration methodologies by reducing inefficiency, overheads, and inaccuracy, ultimately providing companies with a more effective platform to comply with statutory obligations. As the share register can interface with external machine systems there is scope to further automate the process through automatic fillings.

3.7. Legal Smart Contracts

Legal and regulatory considerations have played an essential role in the shaping of the Hypersurface protocol. Smart contracts are neither capable nor appropriate for all situations. When dealing with humans “off-chain”, traditional legal agreements are still the most effective format for encoding such agreements. Hypershare not only consist of its on-chain components, but provides a way of creating “smart legal contracts” where some or all of the obligations are recorded, enforced, and executed automatically by smart contracts, and others are rendered in plain text and enforced using the traditional legal system.

In the simplest sense, Hypershare provides a way of digitising legal agreements so they are machine-readable. These agreements are legally enforceable and can be signed cryptographically and parsed by external machine systems enabling search, analysis, and integration by third parties. Not only does the protocol establish a strong, real-world legal foundation for users, allowing Hypersurface equity to function as

a genuine digital asset (rather than a simple tokenised representation of an off-chain asset), but by providing information in a format that is machine-readable, Hyperframe opens up entirely new avenues for automation.

Structure

The **metadata** records the key terms contained within the agreement in a machine-readable format.

The **markdown** records and captures the terms of the legal agreement in a human-readable format.

The **smart contracts** enforce the relevant terms from the agreement on-chain.

3.8. Metadata

Hypershare uses a metadata model to present the key terms of an agreement in a machine-readable format. Providing metadata on the underlying agreement greatly enhances accessibility for third-party applications by presenting key information from the agreement in a way that can be indexed and utilised by external machine systems.


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

Encoding

The process of creating and encoding legal smart contracts generates a secure link between objects. By creating a bidirectional link that maps the intended relationship between the legal contract and the smart contract in the token URI, the process creates a cryptographically secure integration that ensures that information recorded off-chain is tamperproof.

In this example, we use a token holders agreement. The steps to create a smart legal contract are as follows:

1. The user inputs data via the web application.

2. This data is then used to create a structured metadata model using JSON.

3. A new token is created in the Hypershare token contract with a unique identifier.

4. The metadata model is updated with a reference to the unique identifier of the token.

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 Hypershare token is updated with the structured metadata model IPFS URI.

4. Hyperclaim

Hyperclaim is a decentralised credentialing solution. Hyperclaim allows the Hypersurface community to curate a list of trusted verifiers to provide credentialing services. Using claims, signed digital attestations asserting that an account has some attribute or attributes, users can build digital identities for use in credential-based compliance procedures.

The collision between regulated assets and permissionless protocols presents a unique set of technical, ethical, and regulatory challenges. The blockchain has eliminated middlemen from financial transactions by provisioning solutions directly between buyers and sellers. Although this has created a more efficient and egalitarian ecosystem, it has done so at the cost of massive deregulation. As a result, hacks and rug-pulls are common throughout DeFi.

While regulators have sought to keep pace with the changes taking place in the blockchain ecosystem they have largely failed, instead resorting to public sector conservatism and regulatory crackdowns in an attempt to protect users. Unfortunately, this reactionary approach has fallen short due to the same deficiencies that have often plagued financial markets, many of which drove the design and development of blockchain technology in the first place. High-level controversies surrounding regulated firms such as Celsius and FTX show that even authorisation and oversight cannot guarantee user safety alone.

Instead of reflexively returning to centralised approaches or attempting to downplay the importance of trust, we believe the key is to both acknowledge and integrate traditional legal and regulatory controls in a way that is structured, intentional and consistent with the objectives of web3. Namely, in a way that instills trust for operations that cannot be automated or performed on-chain, while preserving as much of the trustlessness and privacy of the underlying blockchain as possible.

4.1. Digital Identities

As a platform for regulated interactions, digital identities play a fundamental role in the Hypersurface protocol. Identity is crucial in allowing (1) users to engage with one another online with confidence, (2) creating binding legal agreements between parties and (3) enabling smart contracts to validate credentials, thereby automating the process of compliance. With trust secured by a tamper-proof digital environment, compliant parties can participate with greatly reduced friction.

Verifiable digital identities create a powerful resource that enables users to engage broadly across investment, ownership, and governance on the blockchain. Identities are persistent, meaning they may only need to be verified once to open an entire network of opportunities. In this sense, an identity account can be thought of as a digital ID card. Not only is it valid across opportunities, but with further standardisation, it may be used across the blockchain ecosystem.

4.2. Claims

A blockchain account has no value in and of itself. To build a meaningful picture of the underlying user or organisation, an account needs “claims”. Claims can be summarised as cryptographically signed digital statements, attesting that an account has some property or properties. Claims can either be self-attested, signed by other users or signed by a trusted third-party credentialing solution. Claims enable information to be verified near-instantly, allowing smart contracts to read and validate attributes of users on-chain.

Claims enable transfer controls and compliance to be automated and enforced at the protocol level. As more claims are associated with an account an actionable model of identity begins to emerge. Whereas previously, issuers would manually verify who becomes a shareholder, claims enable issuers to specify attributes that shareholders must meet before they are eligible to receive shares. This enables issuers to automate transfers, which we believe will enable greatly enhanced transferability and liquidity for private equity investments.

We expect claims to play an important part in the Hypersurface ecosystem, taking on a more diverse role as the Hypersurface ecosystem grows. Hypersurface aims to establish a global, compliant on-chain ecosystem for private equity investment. However, given the vast scope and subtleties of regulation across jurisdictions, initially, claims will be used as a means of verifying statements in credential-related interactions.

Claim Verification

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

1. AcmeKYC creates a Hypersurface account.

2. Hypersurface verifies AcmeKYC 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: a. Identity verified. b. An accredited investor. c. A citizen of a given jurisdiction.

4.3. Trusted Verifiers

Hypersurface will provide an unopinionated infrastructure platform for an ecosystem of “trusted verifiers”. Verifiers are trusted third parties that provide credentialing services for the Hypersurface ecosystem. In exchange for economic incentives, verifiers may issue claims attesting to the accuracy of a given piece of information. Anyone who knows that a trusted verifier issued a claim can be confident in the veracity of a claim without needing to verify it themselves. Crucially, to maintain decentralisation and preserve its status as an infrastructure platform, Hypersurface will not have final authority over who is admitted as a trusted verifier. Instead, Hypersurface will provide the means for its community to administer the list of trusted verifiers via the HyperbaseVerifiersCurator contract.

HyperbaseVerifiersCurator is, in essence, a token curated registry (“TCR”). The curator aims to establish a fairer and more balanced curation process than regulatory approval, in order to generate a fairer and more balanced ecosystem. The registry uses a set of rules to determine which items are allowed on the list and which are not. These rules are enforced through a voting system where token holders can vote on whether an item should be added or removed from the registry. This system creates a self-regulating marketplace where the value of the token and the quality of the items on the registry are determined by the community of token holders.

4.4. Curation Process

The step-by-step process for how trusted verifier curation works is:

1. Submission

An application is made to join the HyperclaimVerifiersRegistry. This application is accompanied by a number of tokens staked as collateral. The purpose of staking is to discourage spam or malicious submissions.

2. Review

Once an application is made it goes through an evaluation process to determine its eligibility for inclusion in the registry. There is a specified period during which anyone can challenge an application. Challenging provides an opportunity for participants to contest the eligibility of a submission.

3.a. Accepted

If the review period expires without the application being challenged the applicant is accepted and they are added to the HyperclaimVerifiersRegistry. The staked collateral is held in reserve so that the listing can be challenged at any time if the need arises.

3.b. Challenged

If a user has a problem with a particular submission they can challenge its application. To challenge an application a user must stake collateral equal to that staked by the applicant.

4. Voting

Once an application has been challenged, participants in the TCR can vote on whether the item should be added to the registry or not. There is a specified period during which participants can cast their votes. During this participants review the submission, conduct research if needed, and make an informed decision. Each participant can allocate their voting tokens in support or opposition to the submission. The voting power of each participant is proportional to the number of voting tokens they hold.

5. Outcome

At the end of the voting period, the votes are counted and the submission is either accepted or rejected based on the outcome.

6. Redistribution

Once a verdict has been reached, the staked tokens of the losing side and losing voters may be redistributed. This incentivizes honest voting and penalizes those who voted against the majority. For example, winning voters may receive a reward or a portion of the losing voters' staked tokens.

5. Hyperbase

Hyperbase is a lightweight, multi-factor smart contract account that is secure by design. Hyperbase removes private key management from the user experience while maintaining full decentralisation. High-risk interactions are safeguarded by seamless multi-factor authentication, either requiring the approval of multiple devices or the approval of multiple team members.

Blockchain technology today is much like the first generation of the web. While the technical infrastructure is established and capable of supporting use at scale, a relatively small number of key usability issues present a far greater barrier to adoption than the underlying technology. Even in 2022, blockchain applications make little provision for non-technical users. This design philosophy is perhaps best summarised as, “by developers, for developers”.

Although many blockchain enthusiasts are fervent believers in the importance of self-custody, it is important to recognise that for the average user, simplicity is a greater priority than control. It is our conclusion that for blockchain-based applications to achieve mainstream commercial success, the technical infrastructure must be all but invisible to users. Understanding the blockchain must be an optional extra for those who wish to engage on a more sophisticated level, rather than a necessity for anyone who wishes to participate.

In the current paradigm, accounts are made and disposed of at will. Privacy may be of great importance but the throwaway nature of blockchain accounts has prevented the space from evolving. Without being able to make any meaningful assumptions about the person behind the account it has proven impractical to create user-oriented experiences or support registered assets.

Our solution is Hyperbase, a lightweight multi-factor smart contract account. Hyperbase provides drastic improvements over current designs by abstracting all the riskiest, most intimidating, and otherwise inconvenient aspects out of the user experience. Importantly, Hyperbase does so while maintaining the full benefits of decentralisation. This is essential as it ensures that assets belong to their owner and no one else.

5.1 Smart Contract Account

At the core of Hyperbase is a smart contract wallet that functions as a proxy account contract, whereby users may execute transactions. Associated with the account is a key-value store that records an arbitrary number of keys. Any one of these keys may submit a transaction from the account.

Multisignature

To execute a submitted transaction the account requires the approval of at least one other key. The benefit of requiring multiple signatures is that it both reduces the risk of single-point failures and creates a multi-factor authentication process for higher-risk transactions. Users may configure how many approvals are required based on the operation type.

Subdomain Identifiers

Users have come to expect accounts to be identified by names, usernames, handles or email addresses, all of which provide identification in a simple, comprehensible format. Rather than being identified by a 42-character public key, Hyperbase accounts and objects are identified by subdomains, giving users a clear, comprehensible handle for interactions.

Local Keys

To create a simple, accessible experience while preserving self-custody and ensuring that users have direct control over their assets, Hypersurface uses numerous disposable context-specific key pairs. These key pairs are, in effect, standard externally owned account (“EOA”) wallets. Where they differ from standard EOAs is that they are only used to sign transactions locally.

As such, these EOA accounts never hold any funds, which are instead held by the user's core identity account. When a user attempts to access their identity account on a new device, a new key pair is created and stored locally on the user's device. Permission is then requested on the identity account from the existing keys to add the new key. This request must then be approved. Once the key is approved it is added to the account.

Meta Transactions

A significant barrier to the adoption of blockchain-based applications is the requirement for network fees (“gas”) to be paid on any given transaction. Gas fees present a barrier to onboarding as users must first purchase network tokens or hold multiple tokens for a single transaction. Meta transactions, often known as relays, are a powerful mechanism that bypasses the need for the (direct) payment of network fees.

Meta transactions allow users to sign messages showing intent but allow a third-party relayer to execute the transaction itself. A payment in the network token will always be necessary to execute a transaction, therefore meta transactions are not technically gasless, however, they do allow a third party to foot the bill. Hyperbase uses the relay to bypass gas fees on all transactions that are covered externally by its revenue model.

To execute a transaction from a Hyperbase 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 Hypersurface 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: “alice.smith.hypersurf”

A. If the user has an account and key:

1. The local key is used to sign and send the transaction via relay.
2. If the user has an account but no key:
    a. A new local key is generated and stored on the device.
    b. The local key is added as a new signer to a relay transaction.
    c. This transaction is then confirmed and sent from a key with the appropriate permissions. For example, a user may sign the transaction by adding their smartphone from their laptop.

B. If the user does not have an account:

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

6. Conclusion

The Hypersurface protocol has been designed as an open infrastructure for equity tokenisation. The protocol features low barriers to entry and an emphasis on upholding the principles of web3, despite dealing with regulated assets. This plural approach seeks to balance both the risks and benefits of regulation and decentralisation. Accordingly, Hypersurface does not support companies or investors in regulated activities, such as credentialing, investing or fundraising. Instead, the existence of an open, standardised and composable tokenisation service provides a platform for third-party service providers to use, without instantiating them as gatekeepers.

Hypersurface moves beyond a simple equity-management solution, with the aim of creating a digital equity infrastructure. Potential applications, such as secure digital shareholder voting, secondary markets, instant equity-backed loans and on-chain company formation, among many other ideas, have the potential to substantially increase the flexibility, accessibility, and profitability of the global startup and venture finance ecosystems. The concept of an un-opinionated equity tokenisation platform is specific to Hypersurface and provides a platform of unique potential; rather than a siloed, self-contained private databases or highly intermediated centralised broker-dealer tokenisation services, Hypersurface creates an equity value transfer and ownership layer that is well-suited for the global startup and venture capital ecosystem to harness.