HYPERSURFACE

v1.0.0

HYPERSURFACE: DIGITAL EQUITY INFRASTRUCTURE FOR THE INTERNET AGE

0.0

Abstract

Hypersurface is a digital equity infrastructure for the internet age. The protocol provides a suite of tools for issuers to create and manage digital equity assets, and further, allows them to bypass the need for complex administrative procedures, dedicated legal and financial support, and custom token solutions.

Hypersurface uses the blockchain as a transfer infrastructure and secure record of ownership, providing a simple, accessible transactional layer for the global venture ecosystem. Using our technical and legal platform, startups can create and issue digital equity directly to investors and employees. Additionally, Hypersurface provides a number of fine-grain issuer controls and automated compliance verifications, as well an extensible library of legal agreements and modules. Importantly, the protocol is open, interoperable, and comes ready to integrate with external machine systems out of the box.

In this paper we outline the nature and value of the Hypersurface protocol. In section 1 we provide context as to why we believe the protocol is so important. Sections 2 and 3 introduce existing concepts from the blockchain, including decentralised finance and security tokens. In section 4 we outline what we believe to be some of the main barriers to broader adoption. In section 5 we describe the Hypersurface protocol. Sections 6, 7, and 8 introduce the protocols components, Hyperbase, Hypershare and Hyperframe respectively, providing an overview and technical details regarding the technology and its implementation.

1 Introduction **4**
1.1 Vision 4

2 Existing Concepts from the Blockchain **6**
2.1 Decentralised Finance 6
2.2 Tokens 7

3 Security Tokens **8**
3.1 Benefits 8

4 Barriers to Adoption **10**
4.1 User Experience 10
4.2 Intermediaries 11
4.3 Formalisation 12

5 Hypersurface **13**
5.1 Tokenisation Process 15

6 Hyperbase **16**
6.1 Organisation Accounts 21
6.2 Claims 22
6.3 Verifiers 22

7 Hypershare **24**
7.1 Share Register 26
7.2 Compliance 27

8 Hyperframe **29**
8.1 Metadata 30
8.2 Encoding 30
8.3 Electronic Signatures 31
8.4 Modular and Extensible 32

References and Further Reading **33**

1.0 Introduction

In the 21st century, digital systems cut across almost every aspect of organisational and commercial relationships. Computers and the internet have quickly become mainstays in our modern world, yet, from a historical context, they are still in their infancy. While our civilisation has grown 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 a formality, rather than a driver of value. But as a result, even the simplest business procedures often require voluminous paperwork, operations are dependent on a litany of intermediaries and counterparties, and trust is assured by the threat of legal penalties. In venture investment, poor asset transferability is just one example of how these analogue processes hinder effective collaboration and silo value.

On the most fundamental level, a company is an operating system. A control structure that regulates interactions allowing people to exchange value and collaborate toward mutually beneficial ends. When new activities and relationships emerge, new agreements are quickly developed and encoded to regulate them. As such, a businesses legal agreements create an ever-evolving system of controls that match the complexity of the functions they regulate. Equity is just one example of such an agreement.

1.1 Vision

As "software eats the world"[1] and our societies become increasingly interlaced by technical systems, powerful, non-legal mechanisms to regulate interactions have begun to emerge.

In this regard, smart contracts have created a radical new paradigm in business. Like any 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 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 an company to a digital environment, many of the procedures and protocols that make up a business can be rendered and executed automatically.

As the first step on the road toward creating secure, self-executing, programmable business architectures, Hypersurface envisions the development of a new type of shared digital equity infrastructure. A common value transfer protocol that provides a universally accessible system for representing equity assets on the blockchain.

Such an infrastructure would provide an effective transactional layer for the global venture ecosystem, transforming the static, disconnected ecosystem we are familiar with today to one that is open, digital, and designed for the age of the internet. This whitepaper and accompanying protocol offer what we hope to be the first steps toward the emergence of such an ecosystem.

2.0 Existing Concepts from the Blockchain

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 “defence-in-depth”, 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 make use of. In this regard, the blockchain satisfies a need that very few people recognised before its advent: that of an independent digital execution platform. One that is open, accessible, 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. DeFi offers 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 kind 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. Some examples of popular DeFi protocols include:

> Uniswap: A decentralised exchange protocol that allows users to trade tokens without the need for brokers or trusted third parties. At the time of writing, Uniswap has over $928 billion in trading volume.

Aave: A decentralised lending platform that uses smart contracts to allow borrowers instant loans without the need for a bank. At the time of writing, over $11.2 billion in assets are locked into the Aave protocol.

MakerDAO: A decentralised credit platform that supports Dai, a stablecoin whose value is pegged to USD. At the time of writing, over $14.52 billion in assets are locked into the MakerDao protocol.

Although DeFi is still in its early stages, it has the potential to disrupt the traditional financial system by providing cheaper, faster, and more accessible financial services than its centralised counterparts. With minimal barriers to entry and smart contracts enforcing the terms of an agreement, communities of strangers from across the globe can participate in ways that have never before been possible.

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 common categories:

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"[2].

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".

3.0 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 asset value external to the blockchain that grant the holder rights enforced by the law. Such assets may include shares, bonds, and property, among others.

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. Importantly, for security tokens to be recognised and issued as such to investors, they must meet the requirements specified under applicable securities laws 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 with enhanced transferability and settlement.

Securities tokenisation is still a nascent space and has not yet seen large-scale adoption, but is likely to grow in the coming years. This growth will be driven by the significant advantages offered by the blockchain as well as by increasing institutional interest in the underlying technology. A number of major financial institutions, such as the Nasdaq, the New York Stock Exchange, and Goldman Sachs, have already invested in blockchain startups. Venture Capital investment in blockchain reached a record $33 billion in 2021[3]. In addition, a number of countries, including the United States, Canada, and the United Kingdom, are currently exploring the use of blockchain for securities tokenisation.

3.1 Benefits

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

Efficiency

Tokenised assets bypass the need for manual procedures as transactions are settled directly on the blockchain. This dramatically reduces settlement time and enables “24/7” trading, which is not possible via traditional exchanges.

Cost

Blockchain reduces cost for issuers as processes are automated and built atop public internet infrastructure. This eliminates 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 enables compliance to be implemented directly at the protocol level, making it easier to and less error prone to manage and enforce complex procedures.

Liquidity

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 meaningful in illiquid markets, such as venture investment.

Transparency

The blockchain 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 on Earth.

Composability

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

4.0

Barriers to Adoption

However, for security tokens to see wider adoption, there are a number of foundational issues that must be resolved.

4.1

User Experience

Despite its vast potential, the blockchain remains arcane and inaccessible to outsiders. The potential of blockchain technology is increasingly recognised across industries, yet, the common approach to building applications has changed remarkably little since its inception. Even in 2022, blockchain applications make little provision for non-technical users. This design philosophy is perhaps best summarised as “By developers, for developers”.

Application Design

The vast majority of blockchain applications seem more like control panels than consumer-ready apps. Accompanying applications is little in the way of walkthroughs or guidance. While this may be adequate for tech-savvy early adopters or “degens”, for the average user such experiences are generally off-putting.

Addresses

Although 42-character public keys may be easily parsed by machines, to humans they are nearly incomprehensible. If an address is wrong even by a single character then funds and assets may be lost permanently. Public keys contribute to a feeling of overwhelm that is often enough to discourage newcomers.

Pseudonymity

In the current paradigm, accounts are made and disposed of at will. Privacy may be of great importance, however, 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.

Private Keys

Digital wallets are typically secured by a private key that must not be lost or shared under any circumstances. If a user loses or has their private key stolen the funds can be compromised. This creates the essential problem of smart wallet security: a private key must be backed up in case it is lost, but not so much that it may be more easily compromised.

Onboarding

In the blockchain ecosystem, onboarding is almost always tedious and frustrating. Gas fees introduce significant friction to the onboarding process, and KYC procedures often require users to go through a number of additional steps beforehand. In combination with a lack of understanding as to why these steps are necessary, onboarding typically results in a high number of dropouts.

4.2 Intermediaries

Broad financial disintermediation is one of the most important advances introduced by the blockchain. Disintermediation has eliminated middlemen from financial transactions by provisioning solutions directly between buyers and sellers creating a more efficient ecosystem. Unfortunately, the security token space has not kept pace with such advances. Instead of disintermediation, current approaches to building compliant services directly reintroduce gatekeepers.

Extractive

Financial intermediaries create a conflict of interest and introduce unnecessary friction. While these platforms frequently advertise themselves as ‘democratising access to investing’, they rarely transpire to be the great democratising force they assert themselves to be. Typically, such services charge a minimum 5-10% fee on funds raised. This gives them a strong short-term incentive to maximise profits and entrench themselves as volume-based market leaders, often to the detriment of their users.

Opinionated

Intermediaries are opinionated. They conduct due diligence, endorse particular opportunities and charge fees with the aim of turning a profit. This gives them reason to prioritise the opportunities that they believe will generate the greatest return. Unfortunately, this selective approach ostracises large portions of the market. Arguably, the blockchain should provide a transformative platform that is capable of supporting a much broader range of opportunities that may have struggled in traditional markets, such as impact investment.

Disconnected

With centralised services the value offering is based on that of individual companies. Unlike DeFi services, security token platforms compete and scale like traditional businesses. This constrains the growth potential of the ecosystem based on the scalability of their internal procedures (e.g. due diligence, marketing, etc).

4.3

Formalisation

The legal and regulatory system has been slow to modernise in the wake of blockchain. Consequently, there is still a necessary “real world” foundation that is yet to be established.

Compliant

The vast majority of tokens are designed to be permissionless, meaning they can be exchanged freely. However, as with traditional securities, tokenised securities are still subject to regulation and required to conform to compliance standards. The only way to effectively scale regulated assets in decentralised markets is with adequate on-chain compliance controls.

Secure

Token issuers must also be able to perform more sophisticated management operations such as forcing token transfers for legal reasons or fund recovery, as well as freezing and partially freezing tokens.

Machine-readable

Contracts, even in electronic form, legal agreements have failed to keep pace with advances in technology. In the current paradigm legal contracts are rendered in plain text via files such as Word documents or PDFs. Rather than creating a digital version of the underlying data, these documents are recorded in a digital format to capture important information in a convenient, transferable format. Without some type of aggregating framework that presents key information in a machine-readable format, it is extremely difficult for machines to work with the information contained within such files.

5.0 Hypersurface

In the same way that physical systems converge toward the path of least resistance, users naturally tend toward the solutions that offer the greatest convenience. For this reason, unlike its competitors, Hypersurface has chosen to separate the notion of equity tokenisation from equity token offerings (“ETOs”).

Asset tokenisation offers an array of benefits over contemporary solutions. 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. Much like conventional crowdfunding campaigns, what is often perceived as a simple, effective form of alternative funding comes with its own set of drawbacks and considerations.

While the concepts of equity tokens and equity token sales are highly interrelated, they are not mutually dependent. Whereas token sales are dependent on tokenisation of the underlying asset, tokenisation does not demand a blockchain-based public offering as its primary distribution method. ETOs are neither necessary nor appropriate for the majority of users and introduce a litany of regulatory and legal considerations that massively increase cost and complexity.

As yet, there has not been a product that has realised digital equity to its full potential. It is our belief that tokenised equity, as a mature, digital-native asset, is more than viable as a standalone product. Therefore, Hypersurface exclusively targets private, primary market transactions between issuers and accredited investors.

By removing ETOs from the core product offering, issuing digital equity requires very little behavioural change or commitment on the part of users. Whereas tokenisation could easily take several months from end-to-end, without the regulatory and legal concerns that accompany large public crowdsales, issuers may start to see the benefits within as little as half an hour.

Part of what makes Hypersurface’s value offering so compelling is that it is so simple. Instead of manually sharing legal agreements in PDF form, signing them physically or with something like DocuSign, manually updating the shareholder register and issuing share certificates, Hypersurface provides a sophisticated tool for both issuers and investment professionals to streamline their legal, administrative, and transactional activities into a single, integrated process.

In this regard, Hypersurface creates a new digital utility, much like email or file sharing. One that we hope both issuers and investors will come to use on a daily basis. This utility offers what we believe to be a leading-edge solution, not just in the domain of asset tokenisation, but in creating blockchain-based applications for mainstream commercial adoption.

The key distinction between Hypersurface and contemporary equity management solutions is that, rather than using disconnected private records, Hypersurface makes use of the blockchain to create a synchronised record of ownership. One that is open and accessible and can be integrated immediately by other actors in the ecosystem. With ownership and transaction infrastructure secured by the blockchain, information is rendered and available to read and write by anyone with the appropriate permissions. This may be a shareholder transferring shares, or a third-party application.

Open, standardised protocols have been instrumental in the development of many platforms, such as the web. 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 they are. With this in mind, Hypersurface equity tokens have been developed under the ERC-1155 multi-token standard and come ready to integrate with an entire ecosystem of applications out of the box.

From instant equity-backed loans to secondary markets trading and digital voting, the blockchain opens up a whole host of new and exciting use cases. While both analogue and digital equity may represent an equal stake in the underlying venture, digital equity has far greater use value and has greatly enhanced transferability. For this reason, we anticipate the value of Hypersurface digital equity to be greater than its analogue counterpart, and to increase significantly over time as more resources become available.

For a process that takes 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.

5.1

Tokenisation Process

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.

2. Compliance

Define the compliance rules for the asset. This includes: total holder limits, jurisdictional restrictions, jurisdictional 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. The token is deployed on the blockchain. Legal agreements are uploaded to IPFS.

4. Distribution

Invite and issue shares via a private invite link. Investors can create an account in a few simple clicks, review and cryptographically sign digital legal agreements and receive their shares. All in a single, integrated workflow.

5. Management

The share register is automatically rendered, updated, and may serve as the definitive record of a company's shareholders or can be exported to an offline share register. If issuers need to take action they have a suite of tools such as recovery, force transfers and freezing.

6.0 Hyperbase

As a platform for registered assets, identity plays a fundamental role in Hypersurface. 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.

The solution is to use **verifiable digital identities**. 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 is much like a digital ID card. Not only is it valid across opportunities, but with further standardisation, it may be used across the blockchain ecosystem.

Blockchain-based identity accounts enable information to be verified near-instantly by smart contracts. This has significant implications for issuers as it enables the process of compliance and transfers controls to be automated and enforced at the protocol level. With trust secured by a tamper-proof digital environment, compliant parties can participate with greatly reduced friction.

There have been a variety of notable attempts over the years to create digital accounts, all of which have fallen short in one way or another. Ideally, accounts would be secure, self-sovereign, identity-driven, and more broadly compatible with the blockchain ecosystem—all while maintaining the simplicity to onboard first-time users.

Our solution is **Hyperbase**. Hyperbase is a simple but powerful decentralised account model. Hyperbase provides drastic improvements over current designs by abstracting all the riskiest, most intimidating, and otherwise inconvenient aspects out of the user's experience. It does so while still providing the full benefits of decentralisation.

Coinbase, Binance	Hyperbase	Metamask, Rainbow
Centralised	Decentralised	Decentralised
Username	Username (Subdomain)	Public Key
Password	Multi-factor Auth	Private Key
Transaction Fee	Hidden	Gas (Gwei)

In many ways, Blockchain today is 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.

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 necessary pastime for anyone who wishes to participate.

By translating elements of the user experience into design patterns they are familiar with, the underlying blockchain platform is rendered as invisible to users as any component in a web2 tech stack.

	Hyperbase account	Digital wallet	Hardware wallet	Multisig wallet	Custodial account
Secure	Yes	No	Yes	Yes	No
Private	Yes	Yes	Yes	Yes	No
Identity-driven	Yes	No	No	No	Sometimes
Multi-owner	Yes	No	No	Yes	Sometimes
Complexity	Low	Medium	High	High	Low

Importantly, Hyperbase does so while maintaining the full benefits of decentralisation. This is essential, as it ensures that assets belong to their owner and Hypersurface does not have access in any way. This reduces security risk by eliminating administrator access as a potential attack vector.

Instead of expecting newcomers to educate themselves on security best practices, Hyperbase is secure by design. High risk decisions are safeguarded by multi-factor authentication, either requiring the approval of multiple devices, or further, requiring the approval of multiple team members.

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. Subdomains may be created using ENS with the ERC-137[4] or with the newer ERC-4843[5].

Identity Accounts

At the core of Hyperbase is an ERC-734[6] identity account contract. The ERC-734 is a proposed standard for blockchain-based identity accounts, 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, partitioned based on their value and permission level. Any one of these keys may execute transactions from the account in accordance with their permission level.

The ERC-734 EIP outlines several proposed permission levels:

1. Management keys: can make changes to the account.
2. Action keys: can take actions from the account.
3. Encryption keys: can sign messages from the account.
4. Claim keys: can sign claims from the account.

Multi-Signature

The ERC-734 was originally intended for use with singular keys, each with a distinct permission level. However, this introduces a single-point failure to the account structure, as any one compromised key with high permission levels (management, action) could execute transactions from the account.

Multi-signature wallets (“multi sigs”) are a widely used class of smart contract wallets. The benefits of multi-signature wallets are that they both remove single-point failures and create a multi-factor authentication process that is ideal for high-risk or institutional transactions. Hyperbase identity accounts deviate from the standard ERC-734 design pattern in that they are multi-signature by default. Users may configure an optional number of approvals by operation type in order to execute transactions.

Local Keys

While 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. In order 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. However, they never actually become known to the user as they are simply 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, typically from another device. Once the key is approved it is added to the account.

Meta Transaction

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 otherwise, may be required to hold multiple tokens for a single transaction. Meta transactions, often known as relays, are a powerful mechanism that bypass 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.

In order 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 (meta transaction) and submits the transaction to the identity account contract.
5. The identity account contract unwraps the meta-transaction and executes the transaction requested by the user.

User Account Access

To access a user account:

1. The user inputs a personal account subdomain: “bob.hype.surf”
    a. If the user has an account and key:
        i. The local key is used to sign and send the transaction via relay.
    b. If the user has an account but no key:
        i. A new local key is generated and stored on the device.
        ii. The local key is then added as a new signer to a relay transaction.
        iii. This transaction is then confirmed and sent from a key with the appropriate permissions. For example, a user may sign the transaction adding their smartphone from their laptop.
    c. If the user does not have an account:
        i. A new local key is generated and stored on the device.
        ii. A new Hyperbase is deployed to the blockchain via relay, with the local key added as having top-level privileges.
        iii. The user-selected ENS subdomain is registered to the user's account address.

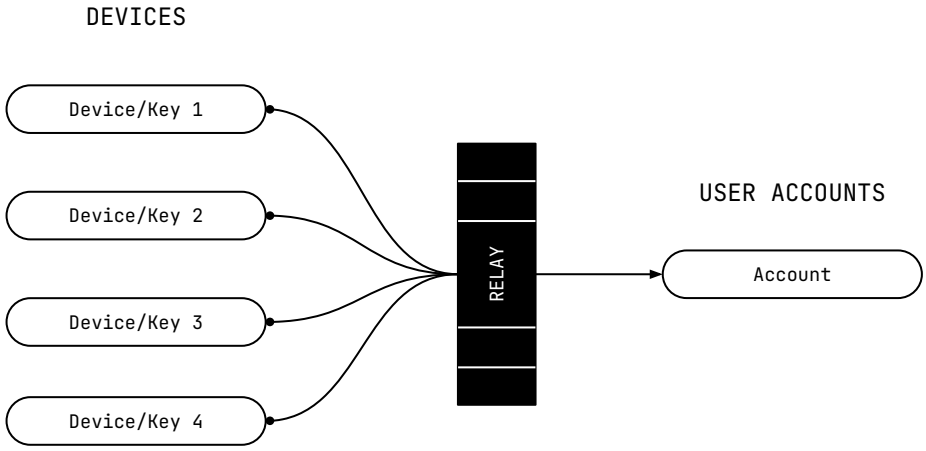


Fig. 1. A number of keys execute transactions on an account via the relay.

6.3

Organisation Accounts

A second layer account may be added to represent organisations. Organisation accounts are added recursively, using individual user accounts as keys. This adds significant additional security. For example, if a user wishes to execute a transaction on an organisation account (requiring action permissions) they may need a second confirmation locally on their own account, validating the transaction on their desktop from their mobile device, as well as the confirmation of one or more team members. Tiered ownership also increases clarity and security as organisation accounts do not need to manage individual devices for each of their users (i.e. Alice's iPhone, Bob's Laptop).

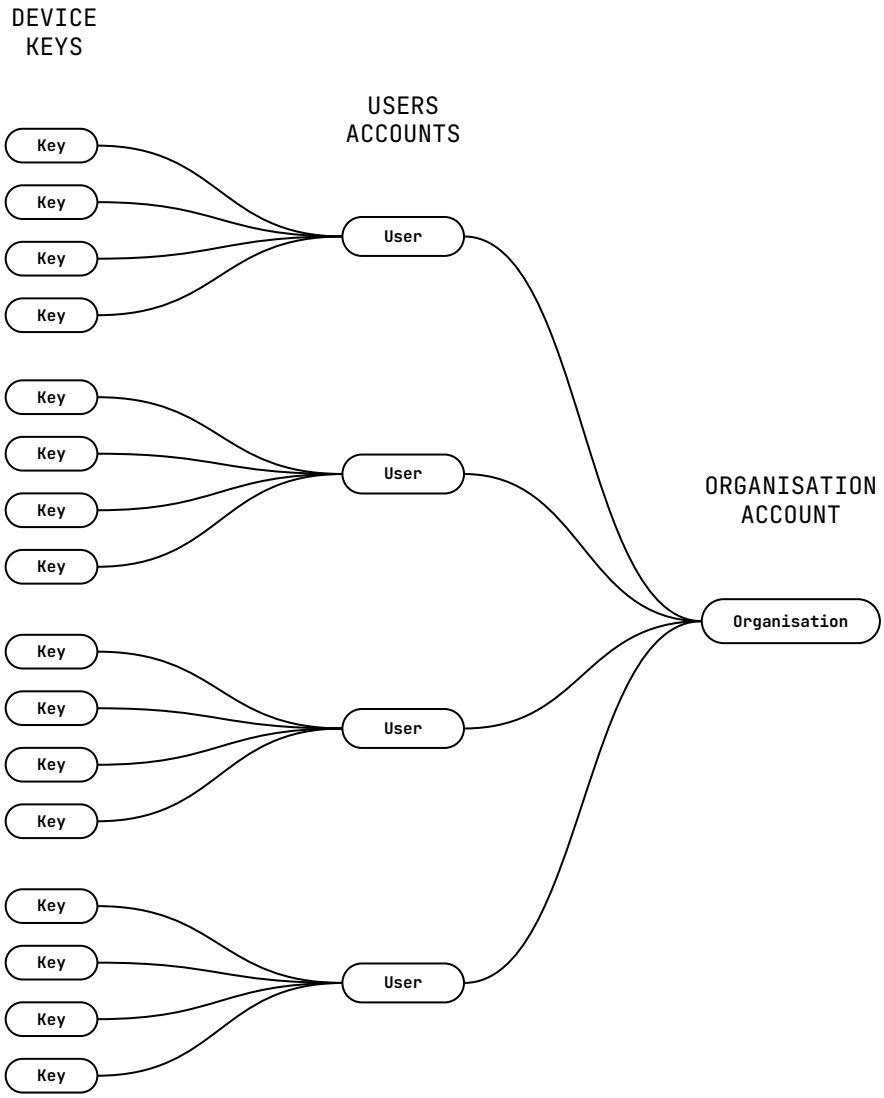


Fig. 2. Multiple user accounts manage a single organisation account. For security purposes multiple signatures may be required to execute higher-risk transactions such as adding new management keys or sending funds to other accounts.

6.4 Claims

An identity 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.

As claims are associated with an account an actionable model of identity begins to emerge. Claims create a powerful resource that enables users to engage broadly across investment, ownership, and governance on the blockchain.

Users may sign claims attesting to statements about themselves or other accounts on-chain. As claim signatures can be linked to the account in question this allows users to verify information about an account without having to store it on-chain or cede it with an intermediary. Such digital 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 something like a digital ID card. Not only is identity valid across opportunities but with further standardisation, it may be used broadly across the blockchain ecosystem.

With trust secured by a tamper-proof digital ledger, compliant parties can participate with greatly reduced friction. Claims enable information to be verified near-instantly, allowing smart contracts to validate the identities of users on-chain. This has significant implications for issuers as it enables transfer controls and compliance to be automated and enforced at the protocol level.

6.5 Verifiers

Hypersurface aims to establish a global, integrated, and compliant venture investment ecosystem. However, with the vast scope and subtleties of regulation across jurisdictions, to preserve its status as an infrastructure platform Hypersurface will work with an ecosystem of “verifiers”. Verifiers serve as trusted third parties that provide credentialing solutions for the Hypersurface ecosystem.

Rather than introducing itself as a bottleneck, Hypersurface will provide a broad platform and marketplace for organisations to verify statements in a formal capacity. In exchange for economic incentives, which may be paid in fiat currency, protocol tokens or other crypto assets, verifiers issue claim signatures attesting to the accuracy of a given piece of information about identity. Anyone who knows that a trusted verifier has checked and signed a claim can be confident in the accuracy of a claim without needing to verify it themselves.

Working with an ecosystem of enables Hypersurface to effectively scale across jurisdictions without having to seek the appropriate licences and approvals for each and every region.

Claim Verification

We expect claims to play an important part in the Hypersurface ecosystem, taking on a more diverse role as the Hypersurface ecosystem grows. However, initially, claims will be used as a means of verifying statements in credential-related interactions. 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 and CDD.
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. The prospective investor pays AcmeKYC and begins the KYC process.
5. After a successful KYC process, AcmeKYC signs the appropriate claims for the prospective investor's identity account.
6. When a share transfer is attempted to the prospective investor the compliance smart contract verifies the receiver's claims and approves the transfer.

Beyond whitelisting, claims serve to add fidelity to interactions, allowing issuers to permit transfers automatically. Whereas previously issuers would have required complete control and would manually verify who becomes a shareholder, claims allow issuers to specify terms that shareholders must meet before they are eligible to receive shares. This enables issuers to automate transfers, which we believe will enable for greatly enhanced transferability and liquidity.

7.0

Hypershare

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. Therefore any design must make remain compliant with legal and statutory requirements. Furthermore, such a solution should provide issuers with a number of fine-grain controls and automations. As such, we identify a number of 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 a shareholders wallet, partially or totally.

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 redeployments of the same contract for each and every new asset, with little to no change between implementations. Needless to say, this is both inefficient and resource-intensive, particularly for use cases such as alphabet shares. Numerous disparate token implementations also increase security risk.

Unlike other permissioned tokens, at its core, Hypershare uses the ERC-1155 multi-token standard. While the ERC-20 requires a new and distinct smart contract for each token, 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 created and added to the list of tokens contained within the contract. This

identifier supplements the unique contract address associated with ERC-20 token implementations. Accordingly, the ERC-1155 features an additional function argument `id` as the unique identifier for each token. Although the contract is shared between multiple tokens, the accounting for each token, operator controls, and compliance controls are kept separate. This approach leads to significant gas savings as compared to that used by the ERC-20 standard, allowing issuers to create new assets at a fraction of the cost and complexity.

Protocol-level 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 an inadequate balance, 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 investor, acquisition, and geographic limits. Somewhat counterintuitively, we believe that stronger transfer controls will increase transferability as without them (a) regulators will not permit large-scale tokenisation of regulated assets, and (b) issuers will not support automatic transfer resolution on-chain.

Advanced Issuer Controls

Hypershare features a number of advanced issuer controls designed to facilitate effective and secure equity tokenisation. In order to do so it is essential that issuers are have options such as freezing assets, partially freezing assets, force transferring assets, and recovering assets for holders. To this end, Hypershare introduces a number of new functions allowing issuers to perform actions, including:

- pause/unpause
- recover
- unfreezePartialTokens/freezePartialTokens
- batchFreezePartialTokens/batchUnfreezePartialTokens
- setAddressFrozen
- batchSetAddressFrozen

Upgradability

Hypershares functional logic may well see numerous upgrades throughout a company's life. To support upgradability, token accounting is separated from the underlying logic. This means that the overall state is maintained between upgrades.

Non-fractional Shares

Non-fractional shares introduce significant usability errors, particularly for services that are reliant on fractional fees, such as liquidity pools. Previous approaches to non-fractional shares simply set to the token to zero decimal places, as opposed to the conventional eighteen. The issue is that this design is hard to reverse once tokens are released into the market. Instead, to support non-fractional shares Hypersurface simply enforces non-fractional token transfers. If a transfer creates fractional shares it will simply fail.

Metadata

In order to give on-chain representation to real-world legal agreements, and do so in a way that is legally and cryptographically binding, the equity token contract must give equal precedent to legal agreements and the corresponding metadata. Hypershare makes use of the ERC-1155's metadata URI to attach a structured JSON legal schema that provides information about the underlying agreement in a machine-readable format. For more information see regarding asset metadata see section 6.

7.1 Share Register

Hypersurface creates a share register with the primary proof of ownership maintained and updated directly on the blockchain. Each share in the share register is represented by an equity token, providing an immutable and secure record of shareholdings and transaction histories. Instead of requiring manual documentation and calculation the share register is automatically calculated and updated on each transfer. To remain compliant the share register must meet the requirements of a traditional share register. Although there are minor changes across jurisdictions, the fields that typically must be recorded are:

- Name
- Address
- Share class
- Number of shares
- Amount paid for shares
- Date person was registered as a member
- Date person ceased to be registered as a member

We believe that Hypersurface's share register alone provides significant benefits over current register administration tools and 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 to provide a platform that automatically submits the necessary fillings when a transfer takes place.

7.2 Compliance

Each and every transfer of Hypershare tokens is coupled with an on-chain validator system. The compliance smart contracts record and enforce transfer controls, ensuring that the transfer and recipient are eligible. Compliance can be used to define and enforce a variety of controls such as accepted countries, the maximum number of investors per country, the maximum number of shares per holder, the accreditation status of the holder and more.

The compliance contracts then read the properties of the asset and interacting identities and enforce certain behaviours, either returning true or false based on the eligibility status of the transfer. When a transfer is made the token contract makes a function call to the compliance contracts to verify the eligibility of (a) the transfer and (b) the receiver. The compliance contracts enforce logic that will check

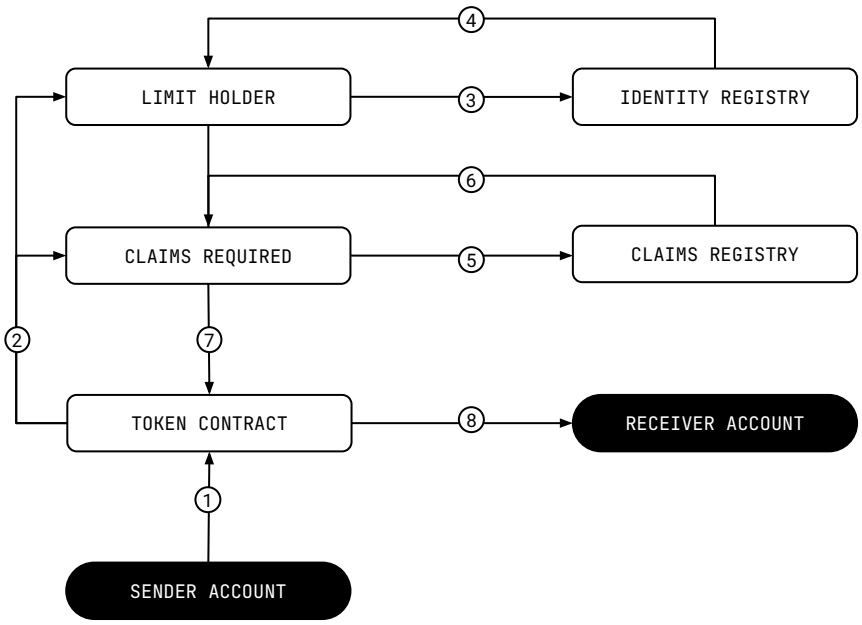


Fig. 3. A user executes an equity token transfer to another user.

1. Sender Account calls the transfer function on the the token contract.
2. The token contract makes a call to Claims Required and Limit Holder to verify the transaction.
3. Limit Holder checks the user is verified via the Identity Registry.
4. Identity Registry returns the status.
5. Claims Required calls the Claims Registry for the users claims.
6. Claims Registry returns the users claims.
7. If both Limit Holder and Claims Required verify the transaction is sound they return “true” to the Token Contract.
8. Token Contract finalises the transfer to the Receiver Account.

the parameters of the token itself such as holder limits and the claims of the receiver's account. Should all requirements be met the compliance contracts will return true approving the transfer, or false otherwise.

The compliance contracts provide an open, programmable means of automating compliance, shifting much of the burden away from users and onto the protocol. This greatly aids in increasing transferability, as in combination with the Hyperbase identity, system much of the menial work of validating KYC and other credentials can be eliminated entirely.

For its initial release Hypersurface is targeting a set of rules and transfer controls that are universally applicable. However, as the protocol grows we hope to be able to add further fidelity to the compliance contracts, implementing new rules in accordance with jurisdictional requirements. With the development of the compliance contracts, we expect to see the emergence of greatly increased liquidity.

Limit Holder

The limit holder compliance smart contract enforces limit-based transfer controls, such as ensuring the maximum number of holders or specific jurisdictional limits have not been exceeded. Limit holder manages frozen tokens, wallets and ensures that tokens are not transferred while paused or in non fractional quantities if required.

Claims Required

The claims required compliance smart contract verifies that the receiver is either whitelisted and therefore exempt, or that the receiver has the appropriate claims to receive equity tokens. Instead of manually checking each interaction the compliance contracts can be used to define essential properties. Claims can be used to verify the properties of an account on-chain.

8.0

Hyperframe

Legal and regulatory considerations have played an essential role in the shaping of the Hypersurface protocol. Needless to say, 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.

Business partners, employees, customers, investors and governments are all broadly recognised as stakeholders. However, if we define a stakeholder as "groups without whose support the organization would cease to exist", then arguably, computer systems are one of the most important stakeholder in almost every organisational and commercial process of the twenty-first century. But while we are heavily reliant on technology, the ability of such systems to interface with our current legal systems is extremely limited.

Hyperframe is the final component of the Hypersurface protocol, it provides a way of creating “smart legal contracts” where some or all of the obligations are recorded, enforced, and executed automatically by a smart contract without human involvement and others are render in text and are the responsibility of humans to uphold. In the simplest sense, Hyperframe is a means of digitising legal agreements so that not only are they secure and accessible, but so they are machine-readable. Hyperframe provides a powerful mechanism to associate smart contracts with legally enforceable agreements that can be signed cryptographically and parsed by external machine systems, enabling search, analysis, and integration.

We believe that this is one of the most important innovations introduced by Hypersurface. 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 approaches to the management of contractual agreements and 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.

A **smart contract** enforces the relevant the agreement on-chain.

8.1

Metadata

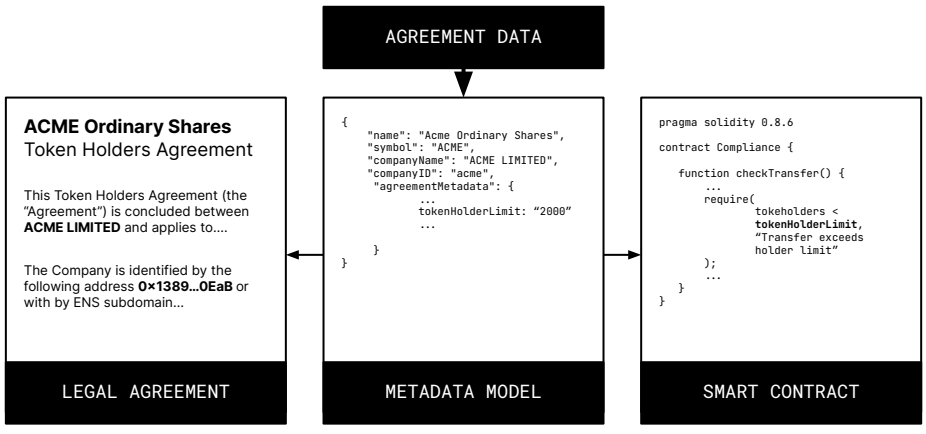
Hyperframe uses a metadata model to aggregate the key terms of an agreement in a machine-readable format. Providing metadata on the underlying agreement enables greatly enhanced flexibility. For Hypershare, metadata is embedded directly in the token URI and structured in much the same way as metadata for an NFT. This aggregates key information from the agreement and provides a way for agreement data to be indexed and utilised by third parties.

```
{
    "name": "Acme Ordinary Shares",
    "symbol": "ACME",
    "description": "Acme limited fully paid ordinary shares",
    "image": "ipfs://QmW78TSUVA2343HCADk..../acmelogo.png",
    "agreement": "ipfs://QmWS1VAdMD353A6SDk..../agreement.md"
    "agreementMetadata": {
        "$class": "org.hypersurface.tokenHolderAgreement.tokenHolderClause",
        "companyName": "ACME LIMITED",
        "companyNumber": "123456789",
        "companyIdentity": "acme.hypersurface.finance",
        "acceptedCountries": ["United Kingdom", "France", "Germany", "Sweden"],
        "signatureRequired": "True",
        "asset": {
            "$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"
    }
}
```

8.2

Encoding

The process for creating and encoding legal smart contracts generates a secure link between objects. By creating a bidirectional connection that maps the intended relationship between the legal contract and the smart contract in the token URI, the process creates a cryptographically secure dual 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.

8.3 Electronic Signatures

In circumstances where signatures are required, blockchain technology offers users increased speed, efficiency, and cost savings over standard authentication processes. The capability to provide secure cryptographic signatures is, arguably, the fundamental mechanism by which the blockchain operates. This mechanism can easily be adapted, providing users with a general-purpose digital signature platform. One that bypasses the need for costly commercial solutions such as DocuSign altogether. Using the blockchain as a general-purpose signature platform reduces the manual task and costs of coordinating signature authentication between parties. As signatures on the blockchain are independent of the underlying agreement they can also be signed in parallel.

To sign an agreement a user simply signs a claim reflecting the relevant fields thereby binding the agreement to their identity on-chain. If signatures are required to participate in certain interactions the corresponding smart contracts can read the claim like any other credential-based interaction and verify the caller is eligible. For example, if an equity token issuer requires that all holders must first sign the token holder's agreement the Claims Required contract will block transfers where the condition (self-signature of the agreement data) has not been provided.

8.4

Modular and Extensible

Hypersurface will feature a library of legal and smart contract modules that can be added to a base contract. The base smart legal contract is intended to represent the minimum agreement between parties. An extensible design pattern is employed to give the issuer maximum flexibility through customisation. Each module extends the functionality of the agreement by adding additional clauses. Through notions of modularity, extensibility, and reuse, Hyperframe enables users to bypass the need for dedicated legal support.

References and Further Reading

1 Why Software Is Eating The World

2 FCA: Guidance on Cryptoassets

3 2021: Crypto VC's Biggest Year Ever

4 EIP-137: Ethereum Name Service

5 EIP-4834: Hierarchical Domains

6 EIP-734: Key Manager

7 Verifiable Credentials Data Model v1.1