Shyft Network Whitepaper

v. 4.1

ABSTRACT

Shyft is a blockchain-based protocol that enables the secure and auditable sending of messages between individual users and trusted parties. Shyft leverages the participation of these parties and their ability to onboard users in accordance with existing compliance, while adding the ability to broadcast attestations of relevant information about user data to other parties by request, assuming user consent is present.

This functionality is intended to facilitate entirely new data marketplaces that empower individual users through an opt-in framework that protects their personally identifiable data. Shyft is built on an amended version of the Ethereum Virtual Machine, optimizing some of its underlying opcodes in order to facilitate a higher transaction threshold and lower transaction fees.

In this document, we explain the thinking that informed Shyft's design, its major components, and how those components work together, We also detail some planned use cases, and lay out our broad development roadmap.

Patent and Disclaimer

The invention disclosed in this Whitepaper is the subject of pending patent applications.

This Whitepaper may contain "forward-looking information". Forward-looking information statements may include, among others, statements regarding the future plans, costs, objectives or performance of Shyft Network Inc. (the "Company"), the ecosystem or the platform or the assumptions underlying any of the foregoing. In this Whitepaper, words such as "may", "would", "could", "will", "likely", "believe", "expect", "anticipate", "intend", "plan", "estimate" and similar words and the negative form thereof are used to identify forward-looking statements. Forward-looking statements should not be read as guarantees of future performance or results, and will not necessarily be accurate indications of whether, or the times at or by which, such future performance will be achieved. The actual results of the Company, the ecosystem and the platform could vary from the forward-looking information contained herein, including as a result of such risks as a collapse in the market for cryptocurrencies, adverse regulatory developments and competition from other platforms. Forward-looking statements and information are based on information available at the time and/or management's good faith belief with respect to future events and are subject to known or unknown risks, uncertainties, assumptions and other unpredictable factors, many of which are beyond the Company's control.

The forward-looking information contained herein was developed based on assumptions related to, among other things, the continued growth of the blockchain technology industry, the success of the participants in the ecosystem and the demand for such participants in the ecosystem and the demand for such participants' product offerings. The Company does not intend, nor does the Company undertake any obligation, to update or revise any forward-looking information or statements contained in this Whitepaper to reflect subsequent information, events or circumstances or otherwise, except if required by applicable laws.

The Whitepaper contains statistical data, market research and industry forecasts that were obtained, unless otherwise indicated, from independent industry and government publications and reports or based on estimates derived from such publications and reports and the Company's knowledge of, and experience in, the sectors in which the Company plans to operate. While the Company believes this data and information to be reliable, market and industry data and information is subject to variation and cannot be and therefore has not been verified due to limits on the availability and reliability of raw data, the voluntary nature of the data gathering process and other limitations and uncertainties inherent in any statistical survey. The Company has not participated in the preparation of such information contained herein.

Introduction

Problem Statement

Since the Internet's inception, one problem has persisted: how can you prove you are who you say you are, and how can you be sure whoever you're communicating with is who they say they are? Or, to put it more simply: how do we trust each other online?

For the engineers and the techno-cultural vanguard that populated the early internet, this wasn't a major concern — if anything, that lack of certainty was a feature, not a bug. As the internet's user base grew, however, the number of communicative purposes its users wanted to port over to it grew, and so its functionality had to try to keep up. This resulted in the development of the password/username framework.

Over time, the weaknesses of this approach became apparent, particularly the fact that it didn't scale well as users had to remember an increasing number of credentials, resulting in users repeating password combinations or resorting to easily-guessable credentials (eg "abc123"). Ultimately password managers came along, both in the form of storage apps like LastPass and, more recently, in the form of major players offloading the work of handling credentials (e.g. Google Authenticator and Facebook). While this solution may currently work for many individuals' "light" identification purposes (email, social media, online stores), the problems are clear: they create highly-centralized stores of user data; very attractive targets for attack. Moreover, these managers don't meet the standards required for "heavy" identification, i.e., passports or a driver's license.

We live in an increasingly networked world, so these features will be offered online in due time one way or another. But who offers them, and how, is of vital importance. As governments and major corporations weigh their options for modernizing heavy ID, the growth of the Internet of Things continues apace, gradually constructing a network of networks, a sort of meta-internet in which all of our most minute actions and interactions become data points that can be accessed by anyone with the ability to exploit security flaws at any of the many points of entry, aka the networked devices.

While the security protocols might well become more sophisticated at the level of individual service providers, your information will only be as secure as the weakest link in that chain of connected services and devices.

In other words, our most sensitive and protected information will be coming online in an environment where our information is paradoxically less secure than ever.

Solution

While the prospect of rampant data insecurity in a hyper-networked world is a frightening one, an effective online trust solution would offer benefits valuable enough to want to weigh those risks.

A solution that offered users and organizations sufficient protections while also providing a framework in which all parties could be reasonably assured freedom from censorship, fraud, and unsanctioned use of shared data could unlock unprecedented scale and new economies of trust online.

To understand what these economies could consist of, let's break down that original problem: "How can we trust each other online?" In this problem, you have (at least) two parties. Let's consider those parties senders. Senders, of course, carry messages - but in the context of the internet, a message could consist of almost literally anything. As an example, consider the Bitcoin network. In the context of Bitcoin, every transaction is simply a conversation between senders, with the message consisting of tokens. In these conversations, "trust" is a matter of simple service fulfilment: do you have the BTC I requested? All other considerations — such as the name of the sender or the time it was sent — are secondary. The BTC itself, as delivered, makes up all the "trust" required. This is able to work because the Bitcoin network leverages its architecture, the blockchain, to make it so that the effort required to dupe a sender would be vastly more difficult and expensive than it would be worth to attempt.

These messages can be thought of as an online counterpart to not only a letter or a bank transfer, but to any process. When you flick a lightswitch, you're sending a message to the lightbulb to change its state from "off" to "on", as determined by the circuit, assuming the presence of an underlying power source. When you plug in and turn your key into your car's ignition, the engine receives a message (electronically or otherwise, depending on the age of the vehicle) to start, assuming there's sufficient gas in the tank, etc. In all cases, the common denominators are: sender, recipient, and the presence of a power structure that enables the process. The difference lies in satisfying the threshold of trust. A lightswitch could be flicked on or off by a human finger, or a stray broom, or a curious parrot. The car's engine, meanwhile, requires that you enter a specifically formatted key. This makes intuitive sense: the car's engine being on or off could have fatal consequences, while the light being on or off is an annoyance at worst, so of course the former's threshold of trust is higher. And yet both processes, in an Internet of Things-assisted future, will be exposed to the very same security risks.

A network that could address these issues would not only address a broad variety of existing security and privacy problems, but unlock a variety of new business use cases and data markets.
We aim to build such a distributed compliance data system—the Shyft Network.

The Shyft Ecosystem

This section describes the major classes of users and a few key concepts that will coexist and interact on the Shyft Network, and how they relate to one another.

Data Holders

Owners of Personally Identifiable Information (PII) as well as non-PII data; this would include individual users providing data about themselves. They may or may not be regarded as Trusted Entities. They provide their data to Trusted Entities in exchange for an attestation. They will make use of app services.

Trust Anchors (Attestors)

Regarded as Trusted Entities. They receive Data from Issuers; review, confirm, and attest to its validity and existence. They hold it off-chain and release it through a private channel following payment of a fee.

Data Consumers

Offer pre-approved app services that require the use of trusted data. They review attestations, determine usability, and request Data from holders.

Nodes (Validators)

Validate and record these interactions as transactions on the decentralized ledger. More on these in the System Architecture section.

Consent Framework

Far too many existing companies and services deliberately obfuscate user privacy options, ensuring that the vast majority of users are never aware of how their sensitive data is being used or sold. This has produced an entire generation of internet users whose valuable data has either been traded for profit or outright stolen as a result of lax security practices.

Shyft is committed to a strict opt-in model, wherein all users have granular control over what personal data they share, to whom, and for what purpose. Users will have the opportunity to change these settings at any time, and UI/UX will be designed to highlight these settings rather than hide them in distant submenus.

Proof of Sender

This is a key concept for understanding Shyft's overall utility, as well as our philosophy to building solutions for both commerce and communication. In the Shyft context, "messages" can consist of any type of data - be it PII or non-PII, individual or aggregated, invaluable or trivial. In the future, these messages might interact more directly with the "real" world,

such as with IoT integration.

None of these interactions would be possible without the Shyft Network's ability to ensure that the Sender of each of these messages provably offers what they claim to be offering — because after all, when it comes to transacting online, proving you have what you say you have is the only measure of "identity" that truly matters. In the context of a Bitcoin transaction, for example, the "truth value" of a transaction consists of no more and no less than the funds appearing in your wallet. All other considerations — the time the transaction took place, the precise address of the other party, etc. — may be interesting or valuable in certain contexts, but they're secondary to the recipient next to the message (the coins) having arrived in the correct amount.

System Architecture

Overview

The Shyft Network is a combination of centralized data attestation and an expansive network of validation nodes that connect to the outside world (the 'Shyft Ring.') The Shyft blockchain features a smart contract-compatible architecture, running simultaneously on the network's bridging technology (Byfrost) and the Shyft Ring.

Byfrost

Byfrost is the network's centralized attestation engine, ensuring data availability and synchronization across the Network.

A software solution maintained at Shyft headquarters and shared as necessary on secure servers, Byfrost is intended to be a connection-of-last-resort for the Shyft Network, in the case of a Shyft Ring consensus failure[1]. It is also a basis for trusted consolidation, accessing a specific randomized merkle hash that will stochastically indicate when there is a desynchronization of Byfrost and Shyft Ring across all mobile use cases.

As a result, any mobile end-user can institute a reliably efficient method of broadcasting these

1For certain classes of users, Byfrost is a Trust assumption for healthy network operation.

desynchronization states across the Shyft Ring's mobile node connection. At the end of every block (17 seconds, with basic timing from the Ethereum blockchain defaults), Byfrost gauges the Shyft Ring's block hash and commits state to Shyft Safe (more on the Safe below) if both are equal.

Shyft Ring

The Shyft Ring is the public-facing Shyft blockchain-enabled software that provides a global consensus mechanism for the state of the Shyft Network. The Shyft Ring connects directly to Byfrost. Shyft Ring participants are necessarily validators for the entire state of the network, completing PoW hashes to propagate blocks and establish security, and may later be upgraded. These validators also act as local connection nodes for non-full-node users.

The Shyft Ring functions exactly like the Ethereum network, barring a few modifications for ease of compliance and Byfrost connectivity. The Shyft Ring also contains a broadcast component that strongly resembles the web API of a block explorer. Every node that receives a transaction passes it to Byfrost and the peers it selects. Uptime is gauged via randomized polling (once per block) of address data.

Each node in the Ring will act as a validator, running a single piece of software that:

- Connects to distributed peers.
- Organizes the deployment of PoW and validation efforts.
- Maintains sparse connectivity to Byfrost to register as a validator on the Shyft Ring.
- Audits Byfrost's work efforts and notifies other peers if there is a desynchronization of state.

Shyft Ring validator participants are incentivized according to the workload distribution necessary for optimal efficiency of the Shyft Network.
Operations that a Shyft Ring validator will facilitate: consensus-based verification of the Shyft blockchain state (in combination with a distributed network of peers), creation of merkle tree Chords by compacting the entire traced tree of transactions per user, and the routing of pre-signed transactions from mobile clients to Shyft blockchain peers.

Chords are created with block hashes as attestation points and function as the primary state verification for incoming mobile requests. Chords allow wallets to resume synchronization with a single hash and allow for a cached data repository on the Shyft blockchain, capable of servicing cross-blockchain initiatives with our ecosystem partners.

Being able to serve from Byfrost (the connection between Shyft Safe and the Shyft blockchain) means that the average transaction time can be reduced significantly and the reward for the Shyft Ring validation process can be appropriately adjusted.

Having the option to KYC the validation nodes would allow at least some institutions to participate in the Shyft Ring, helping further stabilize the network. They would have nothing to gain other than Shyft rewards, as the Shyft Ring cannot modify Byfrost's decision.

Similarly, all nodes that perform attestations would have a heightened inherent ranking. If the consensus fails between Byfrost and the Shyft Ring (i.e. all of the attesting Shyft Ring participants voting against Byfrost's decision), it indicates to the larger network that there is a potential issue with the communication infrastructure between the Shyft Ring and Byfrost.[2]

Shyft Conservators

As the regulatory environment around digital assets matures, the amount of national and regional rules will need to match the existing frameworks regulating how compliance-satisfying data is procured and managed. Building the bridges to connect these regions together is the first step to bring Shyft's benefits to the global market. To monitor such a system without depleting the working capacity of Shyft Ring Validators, we've considered an external (relative to the Shyft Ring) machine learning algorithm trained to detect fraudulent transactions and account behaviors.

Shyft Conservators will operate as Trust Anchors

2 Given that a simultaneous takeover would require the Shyft Ring to immediately grow to a much larger capacity (or else the problem turns into "bad actor(s) also somehow manage to convince all of the good actors to become corrupt at a specific point of time"), the network's own understanding of what the actual proportional vote is for which blocks are valid should show that an issue is about to arise. If consensus looked like 51% vs 49%, there's most likely a problem. if the voting was usually around 10% voting against consensus, to invert it explicitly would require a +80% takeover of the Shyft Ring in a single block to hide that there was an attack.

that can provide an agreed upon service to account holders that wish to have their accounts restricted to their usual purchase patterns. It will also monitor signatures of non-financial data that are outside of the scope of normal activities. This is a basic anti-fraud and identity monitoring service, connected to the Shyft blockchain.

Shyft Safe

The Shyft Safe is smart-contract-powered software that manages and protects certain assets on the network, enabling users' self-custody of these assets. A Safe asset is cross-attested onto multiple blockchains. Here's how it works: A second network, in addition to the Shyft Network, attests to a specific asset. The asset now requires operation on the Shyft Network and the secondary network to be modified, which addresses the "single point of failure" problem.

This is a strategy of long-term bookkeeping that ensures accessibility to assets past the point of last resort of Shyft itself (i.e. certain assets can be spent under some conditions during or after Shyft Network failure). The networks that are used in a Safe asset context need not be of similar smart contract capability. This process only requires contact parameters and metadata, such as a reference number and a pre-signed withdrawal receipt for the delivery of said asset (e.g. from the physical storehouse, if applicable, or, in the case of a digital asset, from a multisignature access account).

System Operation

It is based on the Ethereum blockchain's codebase with the following modifications to its consensus engine:

1. All Shyft Ring nodes must forward end-user requests to Byfrost.
2. All Shyft Ring nodes must validate the transactions in the Shyft Ring mempool up to the defined capacity limit of Byfrost.
3. Uncle[3] generation for Shyft Ring nodes are

3 https://forum.ethereum.org/discussion/2262/eli5-whats-an-uncle-in-ethereum-mining
["Uncles are like blocks that were very close to being the 'correct' next block in the blockchain, but are not because they were resolved after the main block producer. That is why they are uncles and not blocks and constitute a fork in the blockchain, and are thus not valid."] The Ethereum platform rewards "uncles" to add "weight" to the consensus-driven block production.

rewarded identically to the Ethereum model (on a granular depreciating basis dependent on the active computing power of the Shyft Ring node.) Additional incentives for Shyft Ring nodes are to be determined at a later date, and may or may not require a system update.

4. All Shyft Ring nodes must process any end-user transactions, and immediately signal and provide proof to the network of malicious actor activity (for example, attempts to double spend).

All other aspects of the Shyft Network's primary security models closely follow the Ethereum model. As the Ethereum codebase evolves, for instance in its eventual incorporation of the Proof of Stake consensus model, we will keep pace by incorporating technical changes to improve the network.

Initiatives

Shyft's Fuel: The Shyft Token (SHFT)

Use of the Shyft blockchain will require payment with the Shyft token, a "gas" equivalent created to cover the cost of transaction validation, storage of data, settlement, and confirmation.

The term "gas" comes from the Ethereum blockchain, where a single unit of computational execution in the Ethereum virtual machine language (EVM) corresponds to a specific amount of "gas" used. As the Shyft blockchain will initially be an open-source extension of the Ethereum platform, it follows the same mechanisms and uses the same form of payment for services on the Shyft blockchain and the Shyft Dapp platform.

The primary purpose of this gas is to set a predefined price-per-operation for usage of the Shyft blockchain and the smart contracts therein. This sets upper limits on the execution capability of the Shyft blockchain per block generated, creating an opportunity for each validator node to apply an algorithm and charge a specific price-per-operation. In this scenario, Shyft Network participants could potentially collect Shyft tokens and pay on the Shyft blockchain for other services.

Intra-Generational Blockchain Solutions

By leveraging the stability of the Bitcoin network and the smart contract development ecosystem of the EVM programming language, Shyft will develop and maintain blockchain software that bridges the gap between stability and extensibility. This includes potential integrations with sidechain platforms such as Liquid and Rootstock, and the creation and deployment of the Shyft Ring as a public-facing blockchain with transparency, connectivity, and auditability as its primary mandates.

As blockchain technology expands in reach and in scope, we fully expect the development community to find and examine better methods of performing cross-blockchain attestations, as well as the basic software of the blockchains. While the Shyft blockchain initially will be deployed as a Peer-to-Peer (P2P) Proof-of-Work (PoW) blockchain, the longer term goal for the Shyft Network is to upgrade to a distributed settlement system with stronger security guarantees such as a Strong Federation.[4]

Strato Assets

For members of the ecosystem, the Shyft Network acts as a compliance-satisfying, safety-conscious, open-standard operating system. Shyft allows data providers to act as data oracles, enabling high-level connectivity of applications and other services. Shyft will enable developers to run the majority of their private infrastructure on local machines, while architecting applications utilizing Shyft within the cloud. As local machines can also act as validation nodes on the Shyft Ring, the entire network attestation can happen in a distributed, transparent manner—all while conforming to best-in-class encryption standards. Developers can post attestations, state configurations, and registries, powering the next generation of trustless applications.

The Shyft Block Explorer

While Shyft is derived from Ethereum, it avoids one key weakness of Ethereum: overreliance on a single block explorer service. Specifically, the Ethereum ecosystem relies heavily on the block explorer service EtherScan. This creates a "single point of failure" that has the ability to stall or outright cripple many Ethereum-based networks and Dapps if EtherScan itself experiences downtime. If EtherScan were to collapse overnight, many of these same services would be left scrambling for workable alternatives.

On its Mainnet Alpha launch, the Shyft Network will provide a public block explorer. However, it will also provide nodes with the means to host their own block explorers, eventually defraying dependencies across the Network and avoiding the single-point-of-failure issue.

Moreover, the Shyft block explorer has been designed to provide users with a full view of all transactions that take place on the network, including the ability to view details on all individual "internal transactions" that can only be viewed in aggregate on Ethereum block explorers.

Attested Smart Contracts

All smart contracts running on the Shyft blockchain will be signed by their creators. The ability to create new smart contracts on the Shyft blockchain is initially restricted to Shyft developers. The highest quality control standards will be used with careful, secure, and efficient coding practices. All core contracts will be subject to external audits. Once processes and procedures for smart contracts development and deployment for the Shyft Network are established, we intend to open up Shyft Wings. Shyft Wings is a developer program that can be used to post smart contracts from authenticated users. Whether as a company or an individual, users will be able to create software that functions within the context of signature-based smart contract execution in a walled garden environment.

Within the walled gardens, in order to prevent cross-contamination of smart contract event pools and to reduce the risk of harmful contracts, any smart contract design that attempts to store large quantities of the Shyft token (defined below) or another token will be flagged and the application code responsible will go under code review by Shyft developers and bounty programs. While we are at a stage in the evolution of blockchain systems where Dapps such as distributed exchanges are possible and have working examples, we would prefer to initially restrict the usage of the Shyft platform's native token exchange systems. This being said, a "large quantity" here is a measurable value given the Integrated Exchange Valuation score of the tokens with any Trust Anchors serving the price/pair ratio of the tokens. The exchanged value of trades associated with a contract will trigger controls around how that contract is treated, so that large amounts of value don't get locked or otherwise lost.

As the walled garden work progresses, new and innovative applications of, and bridges to, Shyft tokens and the surrounding architecture will arise, enriching and extending the ecosystem.

The Relational Merit Token (RMT)

The Relational Merit Token ('RMT') is intended as a "reputation" storehouse and incentivization mechanism.

The RMT layer, which exists above the compliance layer on the Shyft blockchain, is intended to provide relational data over time for non-vetted participants and give them partial identity and greater access levels, allowing them to use otherwise unavailable services.

RMT would be particularly integral to streamlining KYC/AML compliance and addressing the problem of financial disenfranchisement, two Use Cases we discuss below.

Distribution

This token is distributed based on:

- Initial KYC of a specific address, where the user controls the private key of this Shyft blockchain address
- Positive interactions between attested users
- Positive interactions between Trust Anchor partners, who themselves can also KYC and be rewarded RMT for positive interactions with their user-bases.

Trust Channels

Trust Channels are a form of strong authentication. Application calls to a Trust Channel can be automatically allowed, giving rise to an attestation system that auto-authenticates users for Shyft-verified smart contract services running between any Trust

4 Strong Federations: An Interoperable Blockchain Solution to Centralized Third-Party Risks. https://arxiv.org/abs/1612.05491

Anchors assigned to the Trust Channel[5].

The formation of Trust Channels between Trust Anchors would allow optimal information and transactional flow. Direct trans-institutional transfers of compliance data over Trust Channels solves inter-anchor data siloing occurring on the network, affording even greater cost savings for the institutions.

Note: this is not to be confused with the data siloing of non-blockchain compliance systems we mentioned earlier. This is analogous to how the Lightning Network works around high Bitcoin fees by establishing direct payment channels between peers.

5 The main use case is when a consumer has a Trust Channel alignment through several Trust Anchor and is offered services from other members within the Trust Channel. From a TA/service provider perspective, providing onboarding incentives is easier because the entity is already aware of the payment channels, insurance entities, etc. within the Trust Channel (i.e. no redundant setting up of the channel or diligence conduct.)

Use Cases

Use Case A: KYC/AML Compliance

Recent developments in financial technology require industry participants such as financial institutions and regulatory bodies to quickly adapt to evolving technology or risk major disruption. In some cases, such as inadvertent association with criminal or terrorist elements, failure to keep up can lead to catastrophic consequences[6].
As a result, compliance obligations for financial institutions are increasing in number, complexity, and rigor. Costs of satisfying these obligations continue to rise exponentially. Anything less than strict compliance can result in significant legal penalties and/or reputational damage.

For banks and large institutions, compliance represents a substantial drain on resources. For smaller institutions, it can stifle even basic operations. For example:

- Inefficient compliance onboarding processes cost the average global bank $61 million USD annually.[7]
- Costs in the UK can range from $13 to $130 USD per individual compliance check.[8]
- The average UK bank is currently wasting $6.5 million USD each year due to inefficient manual compliance onboarding processes. This annual waste is expected to rise to $13 million USD over the next three years.[9]
- Financial firms with revenue of $10 billion USD or more spent an average of $150 million USD on KYC compliance in 2017, up from $142 million USD in 2016.[10]

Consequently, financial institutions are forced to cope with maintaining cost-effective, risk-reducing compliance by implementing temporary solutions. The current approach is to simply raise headcount and deploy larger and larger amounts of capital to meet new mandates. This approach is crude, doesn't scale, and has demonstrated diminishing returns:

- In 2013, JP Morgan spent an additional $1 billion by adding 4,000 employees to their compliance department.[11]
- Half of global financial institutions have added employees to keep up with Know Your Customer (KYC) compliance over the past year.[12]
- 75-85% of compliance costs are represented by Anti Money Laundering (AML) spending. The number of compliance professionals deployed to handle KYC increased more than 3.5 times, from an average of 68 employees in 2016 to 307 in 2017.[13]
- Despite significant increases in allocated resources, time required to perform compliance operations continues to lengthen—taking an average of 26 days to onboard clients in 2017, up from 24 days in 2016.[14]
- In 2016, the average time needed to screen a high-risk customer was 5.4 hours.[15]
- AML analysts spend 75% of their time on data collection, and 15% on data organization and entry.[16]

Moreover, compliance processes are often redundantly undertaken by multiple subdivisions of an organization due to "data siloing", thereby multiplying associated costs. Data silos are repositories of data which exist specifically for and remain under the exclusive control of particular divisions of an organization. One division's repository is often inaccessible to another division and/or incompatible with the other division's systems, despite this data being useful to both divisions. These inefficiencies stem from a lack of flexibility and poor interoperability between the organization's

6 https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/financial-services/Facing%20the%20sanctions%20challenge%20in%20financial%20services.pdf
7 https://globenewswire.com/news-release/2017/06/26/1028793/0/en/Typical-UK-bank-will-waste-10m-annually-on-inefficient-KYC-checks-as-AMLD4-regulation-comes-into-force.html
8 https://www.trulioo.com/blog/aml-kyc-automation/
9 http://eprints.lse.ac.uk/79943/1/blogs.lse.ac.uk-Fintechs%20have%20advantages%20over%20established%20banks%20but%20regulation%20is%20a%20major%20challenge.pdf
10 https://uk.reuters.com/article/bc-finreg-beneficial-ownership-rule/banks-brace-for-rocky-implementation-of-u-s-treasury-beneficial-ownership-rule-idUSKBN1D31BK

11 https://www.trulioo.com/blog/aml-kyc-automation/
12 https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html
13 https://globenewswire.com/news-release/2017/06/26/1028793/0/en/Typical-UK-bank-will-waste-10m-annually-on-inefficient-KYC-checks-as-AMLD4-regulation-comes-into-force.html
14 https://www.thomsonreuters.com/en/press-releases/2017/october/thomson-reuters-2017-global-kyc-surveys-attest-to-even-greater-compliance-pain-points.html
15 https://www.thomsonreuters.com/en/press-releases/2017/october/thomson-reuters-2017-global-kyc-surveys-attest-to-even-greater-compliance-pain-points.html
16 The main use case is when a consumer has a Trust Channel alignment through several Trust Anchor and is offered services from other members within the Trust Channel. From a TA/service provider perspective, providing onboarding incentives is easier because the entity is already aware of the payment channels, insurance entities, etc. within the Trust Channel (i.e. no redundant setting up of the channel or diligence conduct.)

technological and bureaucratic systems.

The costs we've described thus far only relate to conducting compliance procedures and not the actual protection of the data procured. As can be seen from widely publicized incidents, data breaches are increasing in frequency and size. Organizations, especially large bureaucratic enterprises, trail behind in the IT security/cybercrime arms race. The 2017

Equifax breach, in which 143 million user records were compromised, is just one example of the potentially catastrophic risk inherent to centralized databases. In our opinion, traditional solutions are fundamentally incapable of addressing these risks.

Attestation and Operation

Certain transactions on the Shyft Network require compliance-satisfying information from users. Users provide their information (e.g. personal data, jurisdictions that user operates in, and other metadata) to a Trust Anchor, which associates the user's signature with that information. This association is posted to a secondary ledger that operates in parallel to the transaction ledger. This association can then be used as a means for third- party application providers to retrieve compliance data via encrypted communication, as needed. Identity of the user is not disclosed, but his or her reputation can be confirmed.

When transactions are being verified for inclusion in the ledger, adequate available KYC information for both the sender and recipient will be a criterion for a valid transaction in much the same way that the outputs of a transaction not exceeding the value of the inputs is a common criterion for valid transactions. Raw datatypes may have converters that are specified, with representations of what raw data has been converted. When raw data is posted unconverted to a blockchain it may be specified in a plain language data field visible to the public.[17]

Open Standards

Initiatives to set standards with an open development procedure have been met with great success in the blockchain ecosystem. For example, 'ERC20' is a common token format that has been readily accepted as the tokenization process of choice on Ethereum.[18]

Given the diverse nature of compliance processes and data points, we will be developing a KYC Matrix to ease participation of Trust Anchors, decentralized/ distributed application ('Dapp') developers. This will also facilitate future-proofing through community involvement.

Furthermore, the Shyft blockchain will include additional virtual machine instructions for smart contracts to check KYC levels for an address. With these additional instructions, token transfers can also be controlled to require suitable KYC. It is expected that most tokens running on the Shyft blockchain will adopt a standard extending ERC20[19] to include function calls testing the validity of transfers and preauthorization for transfers.

Use Case B: Tokenized Tradable Assets

Tradable assets (e.g. stocks, real estate, gold, carbon credits, oil, etc.) are difficult to physically transfer or subdivide, so buyers and sellers instead trade paper that represents some or all of the asset. However, paper and complex legal agreements are cumbersome, expensive, difficult to transfer, and can be difficult to track, resulting in a labor intensive and expensive process.

This holds especially true for precious metals. Gold and silver are hard assets minted or cast by a refiner and distributed for public consumption through a global network of dealers. Most of the physical gold produced today trades on the London Bullion Market and the Shanghai Gold Exchange. Access to trading accounts on these exchanges is prohibitively expensive for the average investor, who is usually relegated to selling his assets to a bullion dealer at a discount to market price. Gold doesn't earn revenue, and incurs storage fees, resulting in a net loss.

Because of these barriers to entry, most investors simply purchase a paper derivative of gold (e.g. futures, ETFs) as they are much easier to trade on traditional exchanges.

But "paper gold" trades at 400+ ounces per every ounce of physical gold that is actually stored in the vault. Because of this high leverage multiple, investing in "paper gold" for long-term wealth preservation is a non-starter as it does not represent real gold ownership. On top of that, "paper gold" is a purely speculative trading vehicle and may open the investor to counterparty risk.

How can investors enjoy the security of insured physical gold ownership yet benefit from monetizing that physical gold on an open exchange so that it can be used? How can investors make their gold productive? We believe that Shyft has the feature set to facilitate a platform to trade tokenized versions of these assets online safely and efficiently, and we are planning an initiative to do exactly this sometime after the Network is launched.

Use Case C: Banking the Unbanked

According to the World Bank, there are 1.7 billion[20] people across the world currently classified as either unbanked or "underbanked", meaning they have no or insufficient access to traditional financial services. In many cases, this means they are permanently disenfranchised from participation in key services and programs most of us take for granted. Access to these services is considered a crucial step to exiting poverty.

While the locations with populations containing high numbers of "the unbanked" tends towards those with income levels the World Bank classifies as "lower-middle income" — India, Bangladesh, Indonesia, Nigeria, and Pakistan all fall under this bracket, for example — the fact of the matter is that we're seeing considerable levels of this type of disenfranchisement even in so-called "first-world" nations. For example, roughly 6 to 7 percent of Americans are counted among the unbanked and underbanked.[21] (This includes some 300,000 residents of Los Angeles alone.)

Individuals who, for reasons of unemployment or underemployment, or merely being located in a so-called "banking desert", find themselves having to rely on alternative banking substitutes such as payday lenders, predatory institutions that charge exorbitant rates with the tradeoff of quick access to some funds. Yet others may find themselves even more fundamentally disenfranchised because the credentials they possess, if any, originate with a failed or failing state, adding a level of what we might call institutional disability. Through no fault of their own, these individuals and families have found themselves with no accessible means to leverage identifying documentation into financial enfranchisement.

For traditional banks, with their rigorous internal guidelines, these individuals simply represent too great a risk. It's true that there is a decent amount of risk when trusting unbanked individuals generally. However, the current situation presents an almost implicit embargo against unbanked individuals. Shyft will enable self-policing, such that less risk-averse institutions would be comfortable offering services to less than ideal KYC'd individuals. As a result, unbanked individuals have greater access to tiers of financial services currently unavailable to them. While many in the blockchain space have discussed the problem in the abstract, we intend to seriously tackle this issue with incentives specifically designed to make the network accessible to them.

We are currently weighing different models for how users with limited or no access to traditional KYC/ AML-satisfying PII could be onboarded to the Shyft Network. One model would involve Shyft partnering with governments (in a manner not unlike our existing partnership with the government of Bermuda) with a significant unbanked population in order to extend a certain amount of no-strings credit to all new users, with each successive transaction or interaction gradually building their Reputational Merit Score (more on this in the Use Case that follows) and offering them access to essential services connected to the Network.

Another model would allow for existing, trusted users to "vouch" for new users that lack leveraging documents. This would be particularly useful for individuals who are relatively well-established but have family members or other close associates struggling with personal or institutional gaps in their

17 The most direct example of this would be the plain language description of the members of a bit field.

18 https://www.ethereum.org/
19 https://theethereum.wiki/w/index.php/ERC20_Token_Standard

20 https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows
21 http://www.microbilt.com/news/article/how-many-americans-are-underbanked-or-unbanked

credentials. There is no reason some combination of both proposed models could not be employed as it suits our institutional partners.

Use Case D: Integrated Exchange Valuation

Financial exchange systems require threshold limits on amounts transacted for a variety of reasons. For example, should the value of a transfer exceed a threshold limit, the transfer needs to be reported to a regulatory body.

For Shyft Network transfers, transfer value is calculated as the exchange rate of the asset being transferred multiplied by the amount of the asset. Trust Anchors then compare this transfer value to their individual or collective threshold limits to determine what compliance action is necessary, if any.

Trust Anchors can agree on and attest to a specific exchange rate and rate variance within a set time period—the Integrated Exchange Valuation (IEV). When transactions are completed by parties on the Shyft blockchain, the IEV of the asset can be checked to determine reportability of the transaction, if there are any Trust Anchors associated with the user's account that define compliance protocols for transaction reporting, and complete additional compliance procedures as needed based on the involved Trust Anchor's attested smart contract suites.

Development Roadmap

Upon the Mainnet Alpha launch of the Shyft Network, the Shyft team will initially focus on the creation and development of ecosystem standards, and branch out its offering from this base.

With our Trust Anchors and other ecosystem partners in place, we will promote the development of open standards across a broad range of attested smart contract implementations. Similarly, Shyft will partner with as many relevant organizations as possible to advance the industry to a point where costs are lowered for all participants.

This development of standards also includes plug-in capabilities like Shyft Envoy[22], where users can subscribe to API services (e.g., forward to wallets) through ecosystem partners, and purchase subscriptions.[23]

Note: The phases below are subject to change as the majority of the development work will require collaboration with ecosystem partners; Network implementation may require additional time. Further details will be released as development progresses.

Phase 1: Focus on security.

- Operational Byfrost architecture, accepting connections, verifying requests to the mobile beta network. Network validator node architecture beta testing.
- Shyft Ring validator node deployment and incentive program initiation. - Shyft Envoy program initiated to integrate and enable other blockchain attestation technologies.

Phase 2: Focus on compatibility.

- Shyft Wings development schedule begins with the focus on scaling the developer base, committing to the education potentials that Shyft provides.
- Wallet architecture updated to include further compatibility with ecosystem providers.
- Identity, Reputation, Federation scores further refined and attributed to increase the community's ability to reduce credit friction and enable integration into traditional wealth management realms.

Phase 3: Focus on reliability.

- Blockchain architecture redesign with the available technology.
- Ecosystem partners, blockchain interconnects, and reputational fungibility are the main factors.

Phase 4: Focus on convertibility.

- Reclassification pass on assets to enable fungibility in the marketplace.
- Clarify "last mile" problem of exchanging 'digital goods' for real goods, using current best practices.
- Engage in developmental talks with partners to consider large scale system integrations.

22 A plug-in architecture that is developed with ecosystem partners. The goal of this standardized interface is to suit the needs of other blockchain approaches to domains that Shyft participates in. Examples would include other blockchain identity projects, which can increase the Shyft user's effective identity score and enable cross-blockchain use cases.

23 Application Programming Interfaces (API) are a series of standards that allow interconnectivity between connected parts of an application development ecosystem.