<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patent and Disclaimer 01</td>
</tr>
<tr>
<td>Introduction 02</td>
</tr>
<tr>
<td>Problem Statement 02</td>
</tr>
<tr>
<td>Solution 04</td>
</tr>
<tr>
<td>Shyft Network: Ecosystem Overview 04</td>
</tr>
<tr>
<td>Creditability 06</td>
</tr>
<tr>
<td>Ecosystem Standards 06</td>
</tr>
<tr>
<td>Shyft Network: Technical Description 07</td>
</tr>
<tr>
<td>Primary Initiatives 07</td>
</tr>
<tr>
<td>The Shyft Blockchain 08</td>
</tr>
<tr>
<td>On Implementing ‘Know Your Customer’ 09</td>
</tr>
<tr>
<td>Attested Smart Contracts 10</td>
</tr>
<tr>
<td>Shyft Fuel: The Shyft Token 10</td>
</tr>
<tr>
<td>Shyft Blockchain Architecture 11</td>
</tr>
<tr>
<td>Other Shyft Capabilities 15</td>
</tr>
<tr>
<td>The Reputational Merit Token: Creditability 17</td>
</tr>
<tr>
<td>Tentative Development Roadmap 19</td>
</tr>
<tr>
<td>Appendix A: BlockUnity Alchemie 20</td>
</tr>
</tbody>
</table>
Please note: The invention disclosed in this Whitepaper is the subject of a pending patent application

Certain of the information contained in 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**

Shyft is a distributed, multi-layer Blockchain-based network enabling users to securely obtain, store, inquire about, and work with regulatory-compliance-satisfying data.

Shyft reduces the costs of compliance due diligence mandates [e.g. Know Your Customer (KYC); Business (KYB); Anti-Money Laundering (AML); Enhanced Due Diligence (EDD), etc.], while maximizing data security and protecting identity beyond the capabilities of traditional, non-blockchain-based compliance systems. In this manner, compliance becomes cheaper, faster, and more secure.

Shyft also features a Creditability system, providing consumers with a reputational score based on compliance and historical transactional activity, which is especially useful for the unbanked.

**Problem Statement**

Recent developments in financial technology require industry participants such as financial institutions and regulatory bodies to quickly adapt to evolving technology or risk disruption and/or catastrophic failure (e.g. terrorism financing).

As a result, compliance obligations for financial institutions are increasing in number, complexity, and rigor.\(^1\) Costs of satisfying these obligations continue to rise exponentially. Anything less than strict compliance can result in significant legal penalties and/or reputational damage.\(^2\)

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.\(^3\)
- Costs in the UK can range from $13 to $130 USD per individual compliance check.\(^4\)
- 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.\(^2\)
- 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.\(^5\)
Financial institutions have 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, unscalable, and, over time, has demonstrated diminishing returns.

- In 2013, JP Morgan spent an additional $1 billion on adding 4,000 employees to their compliance department.\(^6\)

- Half of global financial institutions have added employees to keep up with Know Your Customer (KYC) compliance over the past year.\(^7\)

- 75-85% of compliance costs are represented by Anti Money Laundering (AML) spending. Compliance professionals headcount deployed to handle KYC increased more than 3.5 times, from an average of 68 employees in 2016 to 307 in 2017.\(^5\)

- Despite significant increase in resources, time required to perform compliance operations continues to lengthen—on average taking 26 days to on board a client in 2017, up from 24 days in 2016.\(^8\)

- In 2016, the average time needed to screen a high-risk customer was 5.4 hours.\(^9\)

- AML analysts spend 75% of their time on data collection, and 15% on data organization and entry.\(^6\)

Additionally, compliance processes can be repeated multiple times by subdivisions of an organization due to “data siloing”, effectively multiplying 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 other divisions and/or incompatible with 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 technological and bureaucratic systems.

So far, costs described have concerned conducting compliance procedures and not the protection of the data procured. As can be seen from widely publicized incidents, data breaches are increasing in frequency and size.\(^10\) Organizations, especially large bureaucratic enterprises, trail behind in the IT security/cybercrime arms race.\(^11\) The recent Equifax breach, which compromised 143 million user records is an example of the potentially catastrophic risk inherent to centralized databases. In our opinion, no good (traditional) fix exists.

\(^6\) https://www.trulioo.com/blog/aml-kyc-automation/
\(^9\) https://www.kofax.com/-/media/Files/Infographics/EN/ig_top-5-reasons-you-need-RPA-for-KYC_en.pdf
Blockchain-based distributed ledger technologies have the potential to streamline, cut costs, and reduce risks inherent in traditional compliance systems.

Over the past seven years, projects ranging from digital governance to supply-chain shipping have been developed. Organizations are retrofitting existing product lines with blockchain technology. Proofs-of-concept are appearing in traditionally risk-averse institutional environments to more efficiently mirror vast swaths of data. Additionally, blockchain tokens are being used to incentivize users to act deterministically within ecosystems.

For most - if not all - blockchains currently operating, collection of any user data, let alone collection of data that satisfies regulators is at odds with surrounding ecosystems.

The lack of blockchains focussed on compliance data, coupled with what we saw earlier—financial institutions spending significant resources to tackle compliance—means there is a significant opportunity for a blockchain that automates compliance.

We aim to build such a distributed compliance data system—the Shyft Network.

The Shyft Network: Ecosystem Overview

In this section, we'll introduce some high level aspects of the Shyft Network and ecosystem before delving into the technical details.

Shyft facilitates the accessibility and organization of compliance-satisfying data by leveraging the trustlessness of distributed ledgers and the programmability of smart contracting. In the context of KYC/AML regulations, this powerful combination holds the potential to drastically reduce the resources necessary for compliance.

Functioning as a distributed network, Shyft has no single point of failure susceptible to centralization risk inherent to compliance systems of old, i.e. it cannot be hacked—excluding extremely unfeasible circumstances. Compliance becomes cheaper, faster, and more secure.

The ecosystem surrounding the network is intended to serve both traditional and blockchain-based industries. Startups and established businesses alike participate by providing the compliance data layer, creating and developing applications, or simply consuming network services. Here are some potential use cases:

- **Organizations** seeking to upgrade their costly and risky compliance systems can act as nodes on the Shyft Network (known as ‘Trust Anchors’). Trust Anchors can include financial institutions such as banks, exchanges, or any organization or business for which compliance and KYC/AML processes are an integral part of customer onboarding and maintenance.

- **Application providers** seeking to leverage the compliance data provided by Trust Anchors. Distributed applications can be provided and utilized by Trust Anchors as well as by other businesses where compliance is an obstacle.

- **General consumers** can use the Shyft Network for identification services.
Shyft Ecosystem at a business-interaction (Data Market) level

Data Issuers
Owners of KYC/AML Data. They may or may not be regarded as Trusted Entities. They provide their KYC/AML data to Trusted Entities in exchange for an attestation. Make use of app services.

Data 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 KYC data. They review attestations, determine usability, and request Data from holders.

Nodes
Validate and record these interactions as transactions on the decentralized ledger.
Certain transactions on the Shyft Network require compliance-satisfying information from users. Users provide their information (e.g. the user’s personal information, jurisdictions that the user operates in, and other metadata) to a Trust Anchor, who associates the user’s signature with this information. The association is posted to a secondary ledger that operates in parallel to the transaction ledger. Via encrypted communication, this association can then be used as a means for third-party application providers to retrieve compliance data for regulators and compliance departments as needed. The identity of the user is not disclosed, but his or her reputation can be confirmed via attestation.

Shyft serves a variety of compliance use cases such as financial instrument exchange, crowdfunding, investment, payment, and subscriptions. As regulations, procedures, and new technologies continue to mesh with Shyft over time, arbitration and other capabilities will come online.

Creditability

In addition to lower compliance costs, consumers will benefit from Shyft’s Creditability system. The Creditability system will provide consumers with a reputational score based on compliance data and transactional history, further described in the RMT section below. This is particularly valuable to unbanked consumers, as positive interactions with Trust Anchors in the system contribute to a positive reputational score. For the unbanked, this enables access to other financial services products, which typically require a traditional bank account. Banked consumers will also benefit from Creditability, which offers additional security and faster onboarding when signing up for new services with any Trust Anchor.

Ecosystem Standards

Upon the 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 Anchor and ecosystem partners, 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, where users can subscribe to API services (e.g., forward to wallets) through ecosystem partners, and purchase subscriptions. This will incentivize these ecosystem partners with revenue where applicable (assuming externalized payment processors).

---

12 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.

13 Application Programming Interfaces (API) is a series of standards that allow interconnectivity between connected parts of an application development ecosystem.
The Shyft Network: Technical Description

The Shyft Network is a combination of centralized data attestation (the ‘Shyft Bridge’) 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 Shyft Bridge and the Shyft Ring. 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 the Shyft Bridge.

2. All Shyft Ring nodes must validate the transactions in the Shyft Ring mempool up to the defined capacity limit of the Shift Bridge.

3. Uncle\(^{14}\) generation for Shyft Ring nodes are rewarded on a granular depreciating basis dependent on the active computing power of the Shyft Ring node (with other incentivization(s) to be determined at a later date).

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 Ethereum codebase evolves, we will keep pace by incorporating technical changes to improve the network. The Shyft Network’s subcomponents will be described in the following pages.

Primary Initiatives

Intra-Generational Blockchain Solutions

By leveraging the stability of the Bitcoin network and the smart contract development ecosystem of the Ethereum Virtual Machine (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 via a Strong Federation\(^{15}\) design.

---


[“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]

For members of the ecosystem, the Shyft Network acts as a KYC-based, 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 of assets and indexes, powering the next generation of trustless applications.

The Shyft Blockchain

Pseudonymous blockchains, like Bitcoin and Ethereum, display a limited amount of information regarding the origin, amount, and destination of data. These solutions, while practical for moving value outside the financial system, can be difficult to integrate with services that cannot bypass KYC/AML regulation (e.g. most, nearly all, traditional financial services institutions.) Generally, this is a non-starter for traditional financial service providers, and so this excludes both the institution and its customers.

We propose the Shyft blockchain that facilitates the following: the collection of users’ data off-chain using traditional databases and collection strategies with the ability to provide attestation points for third-party utilization. For example, if a financial institution wants to confirm user completion of KYC requirements in order to participate in a high-value financial transaction, confirmation can be found on the Shyft blockchain. But, this confirmation would not disclose the user’s personal information, mitigating data leak risk.

The Shyft blockchain will allow third parties, or Trust Anchors, to onboard new users and update their data. In order to provide additional security to the entire blockchain, a machine learning system (the Shyft Conservator) is used to investigate and confirm the validity of the information collected through KYC forms.

A compliant KYC/AML system will enable financial institutions and other players to create products (e.g. asset-backed or collateralized loans and debt instruments, ETFs, hedge funds, derivatives, etc.) capturing a filtered target market. Applications on the Shyft blockchain can also extend beyond financial markets; they are limited only to the topology of trust required for execution of a contract.

The Shyft blockchain is the core blockchain software on the various components of the Shyft Network, the Shyft Bridge and the Shyft Ring (described in further detail below). It is an extension of the Ethereum codebase that allows the capability to read and write the attestation data that KYC/KYB data providers require to function, at a protocol level. The primary purpose of this protocol level addition is to achieve a much greater standardization of the formats that are required in the attestation process, along with reducing the transaction execution cost re: lookups to the KYC/KYB database elements.
On Implementing ‘Know Your Customer’

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 data types 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.16

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.17

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. For an illustration of one of the first Dapps being created on the Shyft Network, see Appendix A.

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 ERC2018 to include function calls testing the validity of transfers and preauthorization for transfers.

---

16 The most direct example of this would be the plain language description of the members of a bit field.
17 https://www.ethereum.org/
18 https://etheereum.wiki/w/index.php/ERC20_Token_Standard
Attested Smart Contracts

Attest; be a witness to; certify formally.

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. A formal specification of these practices will be forthcoming as the EVM programming methodologies evolution comes to modern languages and development environments.

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.

Shyft Fuel: The Shyft Token

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 token and pay on the Shyft blockchain for other services.
Shyft Ring

- Functions exactly like the Ethereum network, barring a few modifications for KYC and Shyft Bridge connectivity. Also contains a broadcast component that strongly resembles the web API of a block explorer.

- Every node that receives a transaction must pass it to the Shyft Bridge as well as its selected peers.

- Uptime is gauged via randomized polling (once per block) of address data.

Shyft Bridge

- Connects to Shyft Safe (see more details on Shyft Safe below).

- At the end of every block (17 seconds, with basic timing from the Ethereum blockchain defaults), gauges the Shyft Ring's block hash and commits state to Shyft Safe if both are equal.
Shyft Safe

- Attested Assets (which may include the use of pegged sidechains such as Liquid, Rootstock, etc.)
- KYC data potentially embedded
- Longterm cross-blockchain bookkeeping

The following terms and definitions describe components of the Shyft Network connectivity architecture using the Shyft blockchain.

Shyft Ring (Consensus Mechanism)

Consensus; *group solidarity in sentiment and belief.*

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 the Shyft Bridge. Shyft Ring participants are necessarily validators for the entire state of the network, completing PoW hashes to propagate blocks and establish security (PoW will later be upgraded to a Strong Federation model). These validators also act as local connection nodes for non-full-node users.¹⁹

Shyft Ring Usage

Shyft Ring Validators will run a single piece of software that:

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

Incentives

Shyft Ring validator participants are incentivized depending on the workload distribution necessary for optimal efficiency of the Shyft Network.

Chords

Operations that a Shyft Ring validator will participate in include 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 the 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 a cached data repository on the Shyft blockchain, capable of servicing cross-blockchain initiatives with our ecosystem partners.

¹⁹ There is explicit trust that the connections will not be censored however part of the reward to the validator nodes is based on their honesty (i.e. if a pre-signed transaction is sent to more than one relay/validator node by default and this process is randomized; any node that attempts to censor this communication while another reports to the Bridge truthfully will be penalized by a reduction in reputation and associated rewards as a validator/relay).
Network Performance

Being able to serve from the central Shyft Bridge (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.

Shyft Ring Institutional Partners

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 the Shyft Bridge’s decision.

Similarly, all KYC’d nodes would have a heightened inherent ranking. If the consensus fails between the Shyft Bridge and the Shyft Ring (i.e. all of the KYC’d Shyft Ring participants voting against the Shyft Bridge’s decision), it indicates to the larger network that there is a potential issue with the communication infrastructure between the Shyft Ring and the Shyft Bridge. 20

Within this context, malicious behaviour like double spending should be easy to notice. Registered email addresses of accounts can be notified or any of the double spend transactions can be stopped in place with modifications to the protocol level.

Shyft Bridge

Bridge; something that is intended to reconcile or form a connection between two things

The Shyft Bridge is the centralized Shyft blockchain based attestation engine which functions in tandem with the Shyft Ring to ensure uptime, data availability, and data synchronization.

A software solution maintained at Shyft headquarters and shared as necessary on secure servers, would be running the Shyft blockchain and connecting to pegged sidechain networks Safe attestations. The primary operation of the system is intended to be a connection-of-last-resort for the Shyft Network, in the case of a Shyft Ring consensus failure. 21 It is also a basis for trusted consolidation, accessing a specific randomized merkle hash that will stochastically indicate when there is a desynchronization of the Shyft Bridge and Shyft Ring across all mobile use cases.

As a result, any mobile end-user can institute a reliably efficient method of broadcasting these desynchronization states across the Shyft Ring’s mobile node connection.

---

20 Given that a simultaneous takeover means that the Shyft Ring would need 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.

21 For certain classes of users, the Shyft Bridge is a Trust assumption for healthy network operation.
**Shyft Safe**

Safe; protected from or not exposed to danger or risk; not likely to be harmed or lost.

A Safe asset is one that is cross-attested onto multiple blockchains. 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, removing a singular point of failure.

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 from a multisignature access account in the case of digital asset.)

**Shyft Conservator**

Conservator; a person responsible for the repair and preservation of works of art, buildings, or other things of cultural or environmental interest.

**Intricacies**

As the digital asset regulatory environment evolves, the amount of national and regional rules will need to at least match the existing regulatory frameworks for 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.

**Purpose**

The Shyft Conservator will operate as a Trust Anchor 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.
Other Shyft Capabilities

Trust Channels

Trust; commit (someone or something) to the safekeeping of.

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.

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 Anchors assigned to the Trust Channel.\textsuperscript{22}

\textsuperscript{22} 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.)
**Integrated Exchange Valuation**

Valuation; *an estimation of something’s worth, especially one carried out by a professional appraiser.*

Financial exchange systems require threshold limits on amounts transacted for a variety of reasons (e.g. transfer maximums, reporting thresholds, etc.) 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.
The Reputational Merit Token: Creditability

The Reputational Merit Token (‘RMT’) is intended as a reputation storehouse and incentivization mechanism. The RMT layer, which exists above the KYC layer on the Shyft blockchain, is intended to provide reputation data overtime for non-KYC’d participants and give them reputational identity and access to the KYC layer, allowing them use of otherwise unavailable financial services.

Use Case

The global remittance market presents a great opportunity for RMT. Often remitters (senders) supply KYC data, but remitees (receivers) cannot or do not, as many receivers are considered unbanked, i.e. they lack a bank account and associated financial or credit history. These unbanked individuals are designated ‘Level 0 KYC’ within Shyft.

When remittance services become Trust Anchors to the Shyft blockchain, they are able to allocate RMT tokens to senders and receivers for every remittance transaction. As receivers gain reputation tokens by receiving funds from KYC participants, they can gain trust and access to the KYC layer.23

23 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 enables 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.
Distribution

This token is distributed based on:

1. Initial KYC of a specific address, where the user controls the private key of this Shyft blockchain address

2. Positive interactions between KYC’d users

3. Positive interactions between Trust Anchor partners, who themselves can also KYC and be rewarded RMT for positive interactions with their user-bases. For example, national bank onboarding, where the national bank also would like its users to access Alchemie, an asset-backed token Shyft implementation discussed in Appendix A.

Creditability

Creditability: Applying plausibility, believability, or likelihood that something can be credible, where regular evidence is lacking, like identity and trust. Ability for someone or something to be creditable.

A sender with good reputation transacting with a receiver that may be insufficiently credible due to lack of KYC data or ‘Level 0’ causes the receiver to gain some RMT.

Receivers with low-level KYC and a supply of RMT tokens will gain Creditability over time, becoming more likely to be trusted by institutions in regulated markets, and earning access to introductory financial services. This may allow some as-of-yet unbanked consumers to enter the larger financial market.

As most KYC processes are often focused on the sender, having KYC data and financial history on receivers allows financial services companies to offer new services targeted towards this underserved market or add to existing customer bases, which offer new sources of revenue.

Also, when onboarding these new customers, institutions will have a baseline compliance history on the receiver to help the business decide how much additional KYC is required should the institution and the receiver seek to escalate their business. Institutions can decide to prioritize further investigation on consumers with a low Creditability score (for example, a history of negative interactions between KYC’d users or Trust Anchors) or perform only the required KYC onboarding for those with a high Creditability score.

This also affects banked and existing customers as well. If an existing customer has a positive history overall but frequent negative interactions with a Trust Anchor or KYC’d users, other TAs in the network can monitor the problem customers more closely to prevent fraudulent activity. Trust Anchors can also use this data to give notice to customers that may be at risk of not meeting financial obligations (such as loans, credit lines, etc.)
Tentative Development Roadmap

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

| Phase 1: Focus on security. | - Operational Shyft Bridge architecture, accepting connections, verifying requests to the mobile beta network.  
- Shyft Ring 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.  
- Shyft Conservator program initiated, focusing on first-order financial insurance. |
|-----------------------------|----------------------------------------------------------------------------------|
| 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. |
Appendix A: BlockUnity Alchemie

One of the first Dapps that we intend to introduce on the Shyft Network is Alchemie, which is currently in development by the blockchain production team BlockUnity.

Description

Alchemie is a financial technology platform that offers a series of 1:1 asset-backed tokens and a portfolio of smart-contract-based financial instruments.

Problem Statement

Tradeable 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, yet has 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 longterm 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?

Solution

A series of digital tokens deployed on the Shyft blockchain backed by one unit of a physical asset held in allocated and insured storage in a vault or warehouse.

Use Case

Alchemie expects to launch its initial token, BlockUnity Gold, or BU-Au, on Shyft. The purpose of Alchemie is to enhance liquidity by increasing the transaction velocity associated with physically-backed instruments. As supply chains are further developed, more classes of tokens will be added to the platform (e.g. silver, platinum, etc.) In addition, Alchemie will also feature a portfolio of P2P transactional services that will be gradually expanded and developed.

The platform’s main objective is to create a stable and insured digital asset free from the frictions of traditional financial services, while making assets that are otherwise difficult to move more liquid.
The core advantage of asset-backed tokens is underlying value: the assets’ ability to move in more standardized and well-developed markets. Blockchain technology provides them with liquidity and cost-effective record keeping as trustless distributed ledgers.

The biggest challenge, however, lies in securing supply chain and storage facilities that are both reliable, highly secure, and low-cost. In order to tackle these issues and guarantee the integrity of the digitized assets, BlockUnity is in the process of securing the services of one of the world’s most respected gold and precious metals manufacturers and custodians. BlockUnity is also working with a well-known international precious metal trading platform operating in 25 countries.

BU-Au tokens have all the technical attributes of a digital asset and transact over the Shyft blockchain, but represent real physical gold held on an allocated and insured basis in ISO-certified vaulting facilities in Canada and other global regions users request.

In addition to being able to trade on digital asset exchanges, BU-Au Tokens can be used to facilitate easy P2P investments, trading, or posted as insured collateral for lending transactions on the blockchain.

The price of each BU-Au Token will be directly tethered to the price of gold. This will offer stability to the token and will become useful in hedging the volatility of other “un-backed” digital assets.

BU-Au Tokens will comply fully with FinTrac and other jurisdictions’ regulatory compliance requirements. Although tokens trade freely in the open market via digital asset exchanges, purchasing actual bars of physical gold or taking delivery of physical gold will require full KYC registration either at the point of purchase or at the point of redemption.

Ultimately, BU-Au tokens offer the best features of traditional gold markets by providing the stability of physical gold ownership together with the speed and ease of trading offered by traditional exchange-traded paper markets.

BlockUnity provides an ability to turn what would otherwise be considered a stale asset into a productive and useful asset that can be instantly mobilized globally without ever leaving the vault.

**Entry Point and Asset Storage**

BlockUnity will provide the initial onboarding for interested users. In addition, the Alchemie platform will provide the exchange between CAD/USD/BTC/ETH to BU-Au. BU-Au token holders will have two asset storage options: pool or allocated storage (the latter being fully insured, identified, and stored assets in one of BlockUnity’s supplier’s vaults.) Pool storage is still fully backed 1:1 by physical assets, however these are stored in an asset pool that enables quick and fluid exchange of digitized assets. Users also have the option to redeem their tokens and request delivery of the physical asset, provided they have accrued the equivalent of at least 1 kg of BU-Au. In exchange for use of the platform, users pay service fees.
Smart Contracts

In order to protect BU-Au tokens against theft (e.g. by hacking) and to ensure regulatory compliance, a registry of encrypted KYC information will be maintained as per Shyft Network operation. The smart contracts maintaining ownership records and assessing storage fees will include a function to revert ownership to the last owner in the KYC registry in order to prevent unauthorized transfers to anonymous addresses, as such transfers can be more easily prosecuted.

Hierarchical Deterministic (HD) keys will be used to encrypt individual components of the KYC filings, with copies of the necessary private keys provided to regulators and other government entities as required by law. Jurisdictions that apply to the address owner will be included unencrypted in the KYC registry in order to enable regulators to audit the registry for compliance. Each user’s top-level private HD key for their KYC information, however, will be private to themselves.

Alchemie will also feature an initial portfolio of smart contracts that allow users to send/receive BU-Au, use it as collateral in P2P loans, or integrate asset pools that provide liquidity to exchanges and other services.