Sygna

Sygna is a KYC/AML solution for compliant-minded Virtual Asset Service Providers, individuals, and institutions. Acting as an interface layer between transactions and the blockchain, it functions as validator, publisher, and protector of transactions for both users and providers. It enables a centralized, pollable directory while individuals maintain physical possession of their private keys using joint-custody[1] hardware wallets.

Glossary:
AML - Anti Money Laundering. CFT - Combating the Financing of Terrorism. FATF - Financial Action Task Force. HSM - Hardware Security Module. KYC - Know Your Customer. PII - Personally Identifiable Information. VASP - Virtual Assets Service Provider.

Background

The initial promise of bitcoin that a "purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution" has given the world a powerful new tool to share and exchange value. In practice by real human actors, however, the pseudonymous and anonymous properties of virtual currencies has made it virtually impossible to distinguish bad actors from good actors.

According to reports, in 2018 alone, criminal use of virtual currency accounted for almost $700 million dollars[2] and exchange hacks accounted for a net loss nearly one billion dollars.[3] Terrorist and criminal organizations routinely use cryptocurrency to fund attacks or other illicit activities.[4] Nations currently under sanctions from the UN and the United States find cryptocurrency a convenient sanction evasion tool.[5] Lastly, many companies use cryptocurrency to sidestep capital flight restrictions, engage in fraudulent behavior, or avoid taxation.[6]

Compliance-focused virtual asset service providers (VASP) typically link digital asset accounts with real-life identities, yet activity monitoring and transaction traceability can only be guaranteed from within a VASP itself. Once a digital asset is

[1] Technically full-custody - non-compliance-initiated transactions are initiated by the user, compliance-initiated transactions are initiated by Sygna as a compliance action.
[2] Chainalysis report
[3] CipherTrace report
[4] Treasury Press Release
[5] Treasury Press Release
[6] New York Attorney General Report

withdrawn from a VASP, there is no effective method to trace the transactions to known individuals. There is no systematic means to ascertain whether the beneficiary of a digital asset transaction is a good or a bad actor.

Current tools to track the flow of funds is primarily done through tools that track addresses. Their goal is to create a list of 'blacklisted' wallet addresses. However, this list is easy to circumvent if a user has control over the private keys; a user can simply create an infinite amount of unknown wallet addresses with private keys to circumvent the blacklist. Blacklisting wallet addresses is thus a non-effective measure to combat money laundering or terrorist financing. A transaction compliance system has not been established in the digital asset industry due to the fact that most transactions involve non-KYC'd wallets and industry players have no standardized identity sharing protocol.

This lack of a solution is compounded by increasingly stricter and swiftly moving global regulation, creating urgency among compliance-minded VASPs everywhere. The Japanese Financial Services Agency (FSA) has recently submitted a bill to their legislative body that will bring regulatory clarity to Japanese VASPs. The European Union is proposing that the industry add real-person identities to addresses to promote accountability and reduce money laundering.[7] The Financial Action Task Force (FATF), presided this year by the United States Department of the Treasury, issued recommendations on virtual asset money laundering standards for all FATF-participating countries, encompassing the vast majority of the liquid marketplace.

A common thread amongst these regulatory movements is a general move towards anti-anonymity of virtual currency transactions and greater transparency to identify illegal activities. Regulators are determined to enforce that the industry create solutions to know the originator and beneficiary on all transactions. Despite virtual currency entities not yet subject to global direct enforcement on identification on all transactions, many jurisdictions and bodies have moved quickly to build the means to enforce these standards.[8]

Another problem with the custody of virtual assets is that most users have experienced difficult wallet and private key self-management. These users understand that losing their private keys equates to losing access to their wallet and funds. Third-party private key management relieves the difficulties and risks of self-management, but relinquishes control of the private keys to the third party itself. A system that allows them de-facto full control over their private keys, while simplifying the difficulties and eliminating the risks of self-management will solve many of the difficult usability of previous wallet models.

In this paper, we present how Sygna is able to 1.) prevent the illicit transfer of value via virtual currency, 2.) prevent the theft of funds, 3.) solve a major compliance issue for VASPs, and 4.) eliminate user pain points in the risky self-management of private keys.

[7] EU AMLD5 Report
[8] US FinCEN, the EU, the Philippines CEZA

Solution

Sygna works as a compliance layer: it has wallet-level[9] real-name registration, transaction screening, and address analysis[10] functionalities. Individuals' Personal Identifying Information (PII) are stored off-chain, separate from transactions. Compliance screening is enforced through encryption: user-signed transactions are compliance-encrypted at the wallet level, and cannot be broadcast directly to the network. Screened transactions that pass local compliance checks are decrypted and broadcast, while non-passing transactions are dismissed.

Implementation of this compliance solution is done through three separate entities: "**Directory",** "**CoolBitX"** and "**Trust"**. Each entity has a different role and is separate from the other two to mitigate risks and conflicts of interest. **Directory** provides KYC service, screening, analysis, policing. **CoolBitX** works as an interface for users through hardware wallets. **Trust** handles wallet issuance[11] and recovery services.

Directory

Directory works as the heart of Sygna's compliance system. It provides KYC service, user management, and transaction screening. Users register their *Sygna Card* through the regulation-compliant KYC process, storing PII data in **Directory**'s GDPR-compliant environment. During Registration, **Directory** creates a mapping between a **registered wallet** and a **user's real world identity.** The registration is done at the wallet level using the wallet *extended public key*. By following industry-standard Hierarchically-Deterministic address derivation paths for new wallet addresses, **Directory** knows the identity of all child addresses within the same wallet, while on-chain pseudo-anonymity is maintained (like traditional wallets). Yet all transactions must go through **Directory** before broadcast: **Directory** holds the key to decrypt the encrypted message, generated from the actual user-transaction by wrapping additional Sygna encryption (before it can leave the user wallet). The user cannot broadcast the transaction without **Directory** approval because **Directory** holds the private key to decrypt it. Policing is customizable by design: transactions containing non-registered parties can be aborted, transactions exceeding certain amounts might require an explanation and purpose, and suspicious activity can be flagged, lead to blacklisting or sanctions. Address analysis - built-in through a risk evaluation mechanism - checks addresses during transaction screening. Consolidating existing lists from governments, major cryptocurrency authorities and voluntary users desiring to comply, the address analysis tool functions as a **pollable address analysis API for external parties**, facilitating queries from external entities regarding individual addresses compliance statuses. Sygna benefits from VASPs offering their users the possibility to opt-in to

[9] Different level identity linking (ex: address-level) limits monitoring or validating

[10] Two of the requirements of AML/CFT compliance is to have the ability to "Maintain records and report high-risk transactions and suspicious activities" and "Freezing of transactions and assets"

[11] **Trust** provides seed generation - effectively creating the wallets.

Directory's database: voluntarily providing extended public key and PII enables Sygna-compliance without relinquishing custodianship of keys. This facilitates complying for the VASPs, and demonstrates the user consciously chooses to help with digital asset transactions clarity. Working with authorities and governments, **Directory** can precisely link the real identity tied to a Sygna address, go through its full transactions history and ancestry, updating child transactions and assess both user and the funds within the transaction.

CoolBitX

In Sygna, all elements have different distinct roles to support the user's safe and compliant transacting. **CoolBitX** handles the physical manifestation of Sygna through its own hardware wallet solution called the "*Sygna Card".* The *Card* functions in a similar fashion to the CoolWallet S hardware wallet: it works as a cold wallet with user's private key stored in a Secure Element (SE) chip, in user's physical possession. A paired mobile application (locally paired by the user, using generated digits displayed on the card's e-ink display for original handshake) connects with the card through BLE. Transactions are processed and signed on the *Sygna Card*, in the SE, with the user's own private key - the mobile application relays signed-but-encrypted transactions to the Sygna servers, who process, unpack and publish to the blockchain. The user transacts through his physical *Sygna Card,* granting him hardware-wallet-like security. Neither the compliance part of Sygna (**Directory**) nor the physical representation (**CoolBitX**) have knowledge of the user's private key. *Sygna Cards* come preloaded with private keys and a built-in encryption mechanism to prevent circumventing compliance screening. **Trust** sets up the post-sign mechanism on-card using **Directory**'s Public key, and locks the SE using its own Public key, thereby preventing modification of the SE code by other parties. **CoolBitX** cannot modify or access SE-related content such as private key without involving **Trust**, who must sign any code or modification touching the SE. This has the added benefit of protecting against users trying to extract the wallet private key from the *Sygna Card* itself: The key is in the user's possession, yet cryptographically masked from the user. Since all signed transactions originating from a *Sygna Card* are **encrypted** with Directory's public key, compliance screening is cryptographically assured.

Trust

Trust acts as the ultimate authority within Sygna. In charge of Key Custodianship, System Integrity and Compliance enforcement, **Trust** commands isolation from the rest of the system, and, as the name implies, requires trust. By compartmentalizing it from the Sygna transactional model, **Trust** protects users and system from external and internal attacks. Because of risks associated with custodianship of wallets, **Trust** requires ironclad security. This is achieved by verbose, monitored, defined access protocols, by using a Hardware Security Module (HSM) for key generation and storage, and by limiting normal **Trust** involvement to wallet creation, wallet recovery, or SE code modification.

When a user joins Sygna, **Directory** registers their real ID and requests a new wallet from **Trust**. **Trust**, using a blank *Sygna Card* from **CoolBitX** and following Payment Card

Industry Data Security Standards (PCI DSS) procedures, loads the *Card* with three critical elements: (1) *the wallet private Key,* from which all addresses will be derived from, (2) *the encryption mechanism,* preventing **CoolBitX** from directly modifying SE-Related code and (3) *the post-sign encryption step* (using **Directory**'s public key) which forces transactions to be processed by **Directory** before relaying. Finally, **Trust** provides the generated *extended wallet Public key* and the now ready-to-be-used *Sygna Card* to **Directory**. As the only entity with access to user PII, **Directory** manages shipping using restricted delivery - the target recipient has to prove his identity at the time of delivery. When the user pairs the *Sygna Card* with the mobile application for the first time, **Directory** confirms and hardens the mapping it holds between PII and Wallet-level identities: The user can then transact within Sygna and compliant networks, knowing that all transactions in-network are compliant.

Because **Trust** is not involved in traditional transactions nor connected to the internet, it is compartmentalized out: neither **Directory** nor **CoolBitX** can gain direct access to the user's private key. **Trust** is the only entity in Sygna that has knowledge of the users' private keys. Combining this with existing security measures such as HSM and the on-*Card* encryption mechanism (preventing modification of the SE code), **Trust** ensures the system's integrity, inside and out.

When a user signs a transaction on her *Sygna Card*, the transaction is signed in the SE, then goes through the ***Trust****-imposed* post-sign encryption step which takes the signed transaction and encrypts it using **Directory**'s public key. The transaction is then sent to the paired mobile application and to the Sygna servers, where it will be processed for compliance, relayed or dismissed. **Trust** *effectively* imposes compliance screening of all transactions from the user's wallet, making compliance screening by **Directory** *cryptographically required*.

In the case of a lost or defective *Sygna Card*, the user must reach out to **Directory** and prove his personal identity. **Directory** provides **Trust** the extended Public key of the lost wallet, **Trust** regenerates the wallet keys from HSM, and generates a new wallet loaded on a blank S*ygna Card* from **CoolBitX**. **Trust** transfers the old wallet funds to the newly-generated wallet: This protects against direct attacks on the lost wallet itself. If any fraud/crime is detected, **Trust** can move the funds to custodianship of appropriate authorities. The new card is sent to Directory, which processes its safe shipping via restricted delivery and potentially additional security (multisig lock, supply-chain,...).

Benefits

- **Bank-like Security** - Combining industry best-practice and entities with compartmentalized functions enables a user to experience Sygna like they would a bank. Sygna caters, protects, and supports the user through his account and his personal *Sygna Card*.
- **External Network effect** - Once deployed, Sygna communicates with other compliant entities: a Sygna user who transact with a non-Sygna (compliant) entity will add a new entry to Sygna's **Directory**. Multiple Addresses can then exist under that external user, which will help provide a better global transaction flow representation.
- **Compliance (VASPs) -** Sygna **Directory** serves as a Global Address Directory, freeing VASPs from having to build and maintain some (or most) pieces of a

compliance system, such as KYC, Data Storage and Wire transfer information. This reduces the risks of sanctions and fines from governments, which means peace of mind and an easier job for compliance and law enforcement officers.

- **Opt-In Ready** - individuals desiring a more compliant crypto experience and/or low hassle custodianship can join Sygna on their own: *de-facto* compliance without having to keep track of every transaction.
- **Partial Opt-In** - a VASP user might voluntarily opt into **Directory** oversight, without committing to Sygna's **Trust** or **CoolBitX**. In that case Sygna does not have custodianship of the private key, yet can confirm that the shared addresses belong to said User for future transacting.
- **Centralized Directory** - Sygna offers a public API for external entities to query the Sygna Directory for the compliance status of specific addresses - in a centralized fashion.
- **Customizable Control -** Sygna Partner Service Providers can restrict and shape actual transaction flow *locally*, depending on the compliance rules they want locally enforced by **Directory**.
- **Full AML/CFT Monitoring** - Wallets are linked to real identities through strict KYC procedures, enabling simple, transparent tracing and monitoring of transactions.
- **Secure Key Generation and Management** - Private keys are generated, stored and managed by **Trust** in an EMV certified facility. Functionally, Sygna offers the user a bank-like experience that they are familiar with, managing a user's account and funds, providing him safe tools to transact. Critically, a Sygna user doesn't need to remember or manage his private key or recovery seed.
- **Hardware Wallet Security** - *Sygna Card* functions as a hardware wallet - concealing and safeguarding the private key in the SE, which is used to sign transactions in a hardware-protected environment through strong, Industry-standard security.
- **Off-Chain Identity Verification Layer for Multiple Blockchains** - As more smart contract blockchain platform solutions develop, Sygna helps them build an off-chain Identity Verification Layer. Leveraging HD derivation paths, Sygna is able to provide identity verification for multiple blockchains, meaning Sygna's own digital signature can further be used in smart contracts on different blockchains as a certification of cross-chain interactions.
- **Payment Portal option -** For traditional Point Of Sale (POS) and other payment portals, Sygna is a viable integration option, both for portals and their customers (end users, merchants). The system ensures the compliance of each transaction while the cards' form factor facilitates a natural transaction experience, similar to a credit card.
- **Evolving the Industry** - By helping shape the future of transacting and bringing clarity to the current environment, we build the bridges to the transaction world of tomorrow.

Challenges

Communication with external VASPs - Unless full PII + extended public key is shared to/from communicating compliant VASPs, we only get a transient compliance trace. We

hope to help bring and/or coordinate compliance communication protocol in the field - some work has already started within Sygna to build from existing efforts such as X.509 and others.

Conflicting Directory directives - As Directory adds local compliance rules and handling, conflicting rules might hinder the transaction flows in the network. Care and design considerations should attempt to preemptively address potential conflicts.

Adoption - We want to invite VASPs and individuals to join Sygna, but driving adoption is complex and difficult - many individuals might be offended or reluctant and miss out on the bigger picture or a safe and compliant ecosystem.

Systemic risks - HSM, network load, security breach, privacy concerns, protocol. Sygna offers a technical solution but comes with a heavy overhead and many risks. We understand that a solid system must continue to evolve to address issues over time, and welcome feedback, questions, comments and concerns you might want to raise.

Conclusion

Sygna is by design split into "**Directory**", "**CoolBitX**" and "**Trust**" to have very distinct separate roles and incentives. **Trust** represents integrity, **CoolBitX** protection, and **Directory** compliance. No individual entity will ever have direct access to both user's PII and the matching wallet private key - the responsibilities are very separate by design. **Trust** accesses the private keys but doesn't know who they are associated with, **Directory** has mappings of real-world identity and extended public key, for compliance, but doesn't know the private key; meanwhile **CoolBitX** is blind to both the key and identity - only the user handles both Identity and Private key at the same time - when transacting. This all-in-one compliance platform permits monitoring, transacting, policing - including tools to flag, freeze, block and even potentially reverse transactions. This is achieved from a user-centric platform of integrity, protecting users, sanitizing the blockchain, promoting visibility and communication.

Designed to be malleable, adaptable and with the ability to manage most scenarios, Sygna keeps evolving. Yet the road to mainstream compliance is shared: Compliance is a team sport, and we all are on the same team.