Liquid: Using CORE for Exchanges for Expansion and Business Growth

In late 2018, Liquid - a leading cryptocurrency exchange - approached Unbound Security looking for a way to keep their clients' assets secure while also providing the fast transaction time and asset liquidity to address clients' needs and provide faster response time in executing transactions.

To achieve both security and speed, the exchange needed to move beyond the hassles of offline wallet storage and manual transaction approvals. Liquid was looking for the right technology foundation to meet their aggressive growth goals, while maintaining their strategy of uncompromised institution-grade asset security and service innovation leadership.

Liquid has prioritized security from the outset – never wavering from their strategy of uncompromised security, even when it came at the expense of acquiring clients and new business opportunities.

However, as the demand for faster transaction times increased, the exchange sought to find a way to meet the demands of the market while maintaining the highest security standards available – as well as its stellar reputation. In turn, higher trade velocity would lead to higher trade volumes – scaling the business and providing new opportunities for service provision.

One of the top cryptocurrency exchanges in the Asia-Pacific region
Licensed under the Japanese regulation
Offers both Cryptocurrency and Fiat exchange services
Offers trades for over 150 cryptocurrencies
Company undergoing rapid growth
Company places a premium on protecting client assets

Key Challenges

Blockchain Keys: Not Your Standard Key

One of the critical security aspects for cryptocurrency is protection of the cryptographic keys that literally control these assets and enable digital transactions. Securing cryptocurrencies is different than securing other assets and presents unique challenges:

- One misuse of a key is enough to lose all funds; a malicious actor does not even need to have the key in his/her physical possession in order to gain ownership of the asset. This threat applies not only to outside actors, but also to rogue insiders who may be conspiring to steal funds from within.
- Due to the immutability principle that is inherent in the blockchain design, once a transaction is recorded there are no do-overs. This presents unique issues relating to fraud and anti-money-laundering (AML) protection. To address these challenges, the exchange had previously been using offline wallets to protect its clients' cryptocurrency assets.

Issues with Cold Storage

Reliance on cold storage, while secure, presented operational issues, due to the lack of automation involved in cold storage transactions. Liquid implemented manual processes involving the operations team and multiple approvers to validate each transaction; approved transactions were signed, in an offline location before being broadcasted to relevant cryptocurrency ledgers.

- Manual transaction approval processes were time and effort consuming – slowing down service.
- Transaction approvals did not take place on weekends or holidays, as physical presence of multiple approvers at the offline location was required to sign and broadcast them to the ledger – leading to delays of not only hours, but days.

To improve end-user experience and increase transaction volume, the exchange looked for a way to accelerate and automate the transaction approval and signing process.

Solution

Liquid chose Unbound's CORE for Exchanges not only to increase overall security measures -- but also to rapidly increase trading volumes, easily accommodate new ledgers, and adopt new and in-demand services.

Using Unbound CORE for crypto asset key management and protection, the exchange was able to partially migrate its platform from offline wallets to a secure, software-only, online service.

CORE uses secure multi-party computation (MPC) to implement transaction signing across multiple devices, each holding a random share of the crypto-asset private key. Each device performs part of the computation using their own key share without the full key ever existing in one place.

How it Works

The exchange set a policy of quorum approvals – requiring *m* people and machines of *n* total to approve a transaction on the blockchain.

CORE enables protection of keys by generating, using and managing keys as random shares distributed among the quorum of multiple participants, that operate in segregated technical environments, thus keys never exist anywhere in complete form.

Each participant can use their key share to give their individual approval for a transaction. Bots can be programmed to accept transactions according to policies pre-defined by the exchange; human approvers can accept transactions anytime, anywhere through an app on their mobile devices.

Once enough of the quorum participants respond to meet the quorum policy pre-defined by the exchange, the transaction is cryptographically signed automatically and then broadcast to the relevant blockchain ledgers.

Benefits

- Secure and Flexible Quorum Systems
  - Enable Liquid to create any size quorums and multi-quorums and configurable advanced approval policies. Administrators can adopt any policies and approvers with a few simple steps in the UI.
- Increased Transaction Speed
  - Secure transaction signing in minutes instead of hours enabled Liquid to deliver a differentiated service with the shortest transaction processing time in the market.
- Flexibility and Expandability
  - Liquid can now add new tokens as needed to meet the fast-fluctuating market demands – within hours, and with minimal effort.

Results

- Fast Deployment
  - Liquid was able to meet their aggressive implementation timelines – 2 months from POC to production. There was no need for dedicated hardware such as a hardware security module (HSM) to protect keys. Deployment involved standard servers in the cloud or on-premises and approvers' mobile devices.
- Increased Operational Efficiency
  - Approvers can now approve from their mobile phone apps – at any time, on any day. There is no physical access to cold storage required. Transactions are processed within less than a minute instead of hours or days (in case of weekends or holidays).
- Business and Revenue Growth
  - Sharp increase in transaction volume due to shorter transaction processing times.

"We are constantly innovating the Liquid platform to give our customers the highest degree of speed, flexibility and convenience while maintaining our pristine record of uncompromised security. Working with Unbound we have successfully enabled secure cryptocurrency withdrawals in minutes, leveraging MPC technology to validate transactions according to advanced security policies in a quick and efficient manner. The robust, tested and vetted technology delivered by Unbound, coupled with high responsiveness and professionalism of the team, helped us go to market quickly."
-- Seth Melamed, Chief Operations Officer at Liquid Group Inc.

About Unbound Security

Unbound Security is the global leader in cryptography and empowers enterprise customers worldwide to confidently secure, manage and authenticate all critical business transactions, information, identity, and digital assets – anywhere, anytime. Unbound Security CORE is the enterprise platform of choice for secure key management, trusted by many of the world's largest banks and Fortune 500 companies. Unbound Security is a recent recipient of the Deloitte Fast 500 award and is headquartered in New York, with research and development facilities in Tel Aviv.