Getty Images

SECURITY > STRATEGY

Liquid Cryptocurrency Exchange Uses CASP to Improve Security, Speed

The cryptocurrency exchange was getting complaints about the speed in which it was processing transactions, until it chose to standardize on a Crypto Asset Security Platform.

Karen D. Schwartz | Jan 31, 2020

Investors have been making a killing by trading in cryptocurrencies over the past exchanges. Without ironclad security, these exchanges are vulnerable to cryptocurrency thefts, fraud and scams. According to one recent report, these types of breaches totaled more than $1 billion in the first quarter of 2019 alone.

Security has always been top-of-mind for Liquid, one of the top cryptocurrency exchanges in the Asia-Pacific region. Since its formation in 2014, the company has grown significantly; it now offers trades for more than 150 cryptocurrencies and continually looks for ways to improve both security and the customer experience.

For the first several years of its existence, Liquid was a "cold wallet" shop. Cold wallets are offline wallets that protect customers' cryptocurrency assets. In the case of Liquid, the private key was fully air gapped from the internet at all times.

By 2017, it became clear that the cold wallet method, while fully secure, simply didn't provide the level of service Liquid needed to sustain rapid growth. One of the major issues was speed; the blockchain-centric service was bogged down by manual transaction approval processes and the requirement for multiple people to physically gather in the same location to approve individual transactions.
"We couldn't process withdrawals fast enough to keep up with client expectations. The speed issue was even making some clients start to doubt our security," said Seth Melamed, Liquid's head of business development. "At one point, I was on the train going to work and got a message from someone saying that it had been two hours since he placed a request for a withdrawal, and calling us scam artists because it hadn't gone through yet."

Time for Something Completely Different

That perception of lax security, plus the need for faster service, spurred Melamed to look for something different. At the same time, he wanted a more distributed, said.

After a lot of detective work, Melamed chose to standardize on the next generation of Liquid's technology on a Crypto Asset Security Platform (CASP). CASP is a bank-grade security platform designed to protect blockchain transactions. In Liquid's case, Melamed chose a Unbound Technology's CASP model with multi-party computation (MPC), which splits information into multiple bits distributed across multiple entities.

"We were pretty close to going in a different direction when someone recommended this approach," Melamed said. "It took us a while to get comfortable with it, but the more we dug in, the more we realized there was no other way to do it. It meant we wouldn't be tied to hardware and there would be no security compromises."

Unbound Technology's CASP uses 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. The Unbound CASP system works in tandem with Liquid's own artificial intelligence-based system that evaluates risk and creates risk policies.

While the bulk of Liquid's assets are still kept in a cold wallet for the time being, the company has begun moving a portion of its digital assets to Unbound CASP vaults. When a user makes a withdrawal request, the system first runs Liquid's risk management algorithm, checking to see whether it is an acceptable risk. Once approved by the risk system, it is sent to the Unbound CASP for secure signing and processing.

gone from the very bottom to the very top," he said. "Once we're at scale, we have all of the risk management tools necessary to support on-demand service levels, even for large amounts."

In addition to the speed and security benefits, Melamed said he likes Unbound's ability to support large numbers of blockchain protocols. Liquid current supports about 35 different blockchain protocols, but is adding an average of about one per month.

While most of Liquid's portfolio is still in cold wallet, the company has become such a big fan of CASP that it is considering abandoning cold wallet completely.

"I believe the CASP architecture is more secure than even our cold wallet; there are less points of failure, but it still has the ability to retrieve the private key if something goes wrong with CASP," Melamed said. "It's not that anything is broken. I just feel we can go to a new level."

0 COMMENTS

RELATED

Synopsys Combines App Testing Tools to Speed Flaw Remediation

FEB 13, 2020

Azure's Hardware Security Feature Takes Cues from Xbox One

JAN 30, 2020

Say Goodbye to Windows Server 2008 – and Hello to Azure?

JAN 07, 2020

Former White House CIO Shares Enduring Security Strategies

NOV 20, 2019

© 2020 Informa USA, Inc., All rights reserved