Liminal Shorts

5 ways crypto exchanges can safeguard their funds

Table of contents

Early Days Of Digital Asset Trading

Ever since the inception of digital assets right from Bitcoin to a scale of new tokens being formulated on the backbone of blockchain networks like Ethereum, the proposition of buying these assets, keeping custody and selling them wasn't as simple as it seems today.

Peer-to-peer transactions and self-custody were the only options available at the early times and they required a certain technological understanding and learning curve to skillfully trade. But as the value interest of these assets started to increase, more and more investors started to share their interest in buying, selling and trading these assets for sizable profits.

Some initial trades started to pop-out on community forums like Bitcointalk, conducted through paypal. And soon enough, reports of deceiving incidents started to happen because of the anonymity involved in the deal and the nature itself of Bitcoin, seen and understood only through an alphanumeric address.

As the incidents started to rise, to become clear there needs a middleman, atleast at this stage of cryptocurrencies to facilitate trades between buyers and sellers, still maintaining their privacy and pushing their trust in third-party operations to close the deal.

Why Exchanges

Overseeing the absence of a dedicated platform to support the trade of cryptocurrencies and the over-bearing response from payment gateways to support cryptocurrency related payments, Jed McCaleb introduced Mt.Gox marking the creation of the first ever Bitcoin trading platform.

This led to a movement of cryptocurrency exchanges opening up with the motive of simplifying the investing process for the layman with a rather easy user-journey.

- Exchanges made price discovery for the available cryptocurrencies efficient to the point that it made the same experience of buying stocks online

- Exchanges allowed users to instantly create their account, link their banks to deposit fiat currency and buy any cryptocurrency

- Exchanges also solved the problem of the custody of the assets bought by the users, as they help responsibility of storing the private key for all of users wallet address where their respective assets were stored

- Exchanges kept instant liquidity to process transaction without delays and offered the most competitive prices for the assets, keeping marginally low commission fee

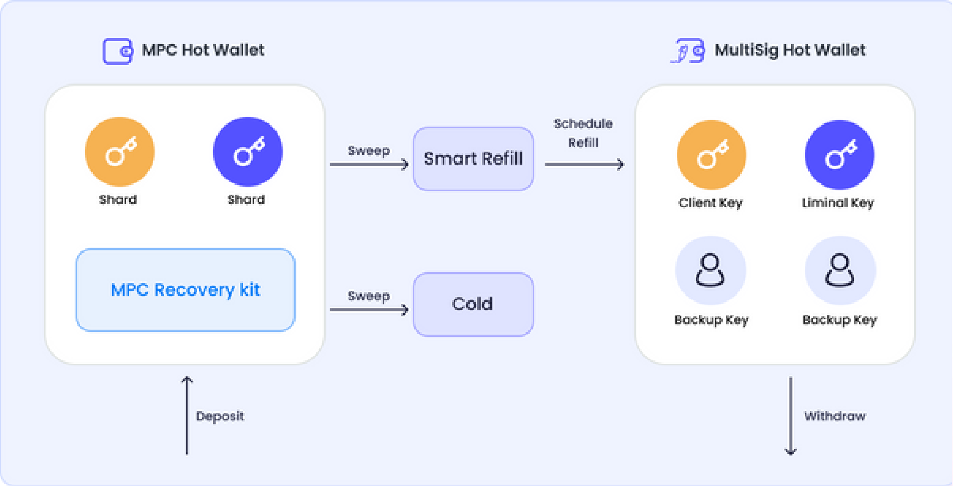
Further in the journey, as more decentralized applications surfaced; their utility token, protocol-native stablecoins, liquid staking tokens entered the market extending exchanges ecosystem, listing inventory and trading variables. This coupled with the massive hype built around altcoins drove exchanges as not just the first point-of-contact to conduct trades but to secure asset custody as well.

What are Hot Wallets?

Hot wallets are special cryptocurrency wallets that provide automated transaction signing capabilities at scale, from within a secure environment. In any crypto exchange infrastructure, withdrawal hot wallets are tasked with the responsibility to process all user-requested withdrawals. Since all transaction requests need to be processed immediately for an optimal user experience, the private keys of hot wallets are always maintained online, making them readily accessible for signing transactions.

Hot Wallets - Exchange pipeline

Anatomy of the Hot wallets. Choose from both MPC and Multisig. MPC recommended on EVM chains.



Hot Wallet architectur | Source - Liminal Research

Few important characteristics of Withdrawal wallets

- Withdrawal hot wallets must have efficient fees estimation capabilities to optimize transaction costs and prevent unnecessary exorbitant fee payments on transactions.

- They should have an efficient transaction queue management system to prevent transaction backlogs, which would otherwise result in a long queue of pending transactions to negatively impact the customer experience.

Hot Wallets and their vulnerabilities

Hot wallets, which are online cryptocurrency wallets that are connected to the internet, are vulnerable to hacking and other security threats. Because they are always connected to the internet, they are more susceptible to cyber attacks, which can result in the loss of funds. In addition, because they are often used for day-today transactions, they typically hold a smaller amount of cryptocurrency, making them less attractive to investors who require larger amounts of funds for trading.

One of the primary ways that hot wallets are vulnerable is through phishing attacks. Hackers will create fake websites or emails that appear to be legitimate, asking users to enter their private keys or passwords, which can then be used to gain access to the user's wallet. In addition, hackers can also use malware to gain access to a user's computer or mobile device, allowing them to steal their private keys or other sensitive information.

Another vulnerability of hot wallets is the risk of exchange hacks. Many cryptocurrency exchanges use hot wallets to store the funds of their users, making them a prime target for hackers. In the event of a hack, users may lose their funds, as the exchange may not have sufficient insurance or reserves to cover the losses.

Furthermore, due to the relatively small amount of funds stored in hot wallets, users may miss out on trading opportunities. If a user does not have sufficient funds in their hot wallet, they may not be able to take advantage of a favorable market condition, resulting in missed trades and lost profits.

Overall, while hot wallets are convenient for day-to-day transactions, they come with a higher level of risk than cold wallets, which are offline and therefore more secure. It is important for users to take appropriate security measures, such as using two-factor authentication and regularly updating their software, to minimize the risk of hacks and other security threats.

Major Hacks Across Centralized Exchanges

Now, most of these exchanges were running into troubles as they ran in an unregulated time, failing to follow the basic norms of security, regulation, compliance and solving the operational inefficiencies and working under false pretense.

It isn't a coincidence that the very first and one of the most successful Bitcoin exchanges got hacked, where hackers drained their key wallets, addresses associated with Mt. Gox's private keys.

In the paradox of crypto security hierarchy there are three main layers; protocol, exchange and personal wallet security. Protocol level vulnerabilities are complex in nature and personal wallets distributed, hence exchanges become an easy target. Holding huge amounts of assets in consolidated wallets makes them more susceptible to hacks and security issues.

According to a study by coinjournal.net 42% of cryptocurrency exchanges either failed or disappeared since 2014 and only 22% were able to survive. Out of several different reasons for these exchanges going down, a cumulative 35% of failure happened because of regulations, hacks and operational breakdown.

Exchanges being a centralized entity, have a single point-of-failure and have inherent vulnerability in their design language. Right from their API integrations to data repositories, hot and cold wallets need to be protected explicitly.

5 Ways Crypto Exchanges can safeguard their funds

Mt.Gox Hack, 2010

Bitcoin worth **$8.75 million** was stolen

Mt.Gox Hack, 2014

$615 million were siphoned off
Site's source code compromised

Bitfinex Hack, 2016

Coins worth over **$60 million** stolen
Coins that were stolen had been moved from one wallet to another to mask a trace-back

Upbit Hack, 2019

Over **$45 million** stolen in a single transaction. Hackers moved a majority of the crypto to other wallets

BINANCE Hack, 2019

Hackers withdrew over **7000 bitcoins** from its hot wallet. Attackers managed to break into the exchange's security systems, obtaining key information sets, including two-factor codes, APIs, and other data

Kucoin Hack, 2020

$281 million worth of coins and tokens stolen. Hackers managed to obtain the keys to some of the hottest wallets on the exchange

Date	Exchange	Stolen Cryptocurrency	Amount Stolen (USD)
Aug 2016	Bitfinex	Bitcoin	$72 million
Jul 2017	Bithumb	Ethereum, Bitcoin	$31 million
Dec 2017	NiceHash	Bitcoin	$64 million
Jan 2018	Coincheck	NEM	$530 million
Jun 2018	Bithumb	Various	$30 million
Jul 2018	Bancor	Ethereum	$23.5 million
Sep 2018	Zaif	Bitcoin, Bitcoin Cash, Monacoin	$60 million
Jan 2019	Cryptopia	Various	$16 million
May 2019	Binance	Bitcoin	$40 million
Jun 2019	Bitrue	Various	$4.3 million
Sep 2019	Upbit	Ethereum	$49 million

Date	Exchange	Stolen Cryptocurrency	Amount Stolen (USD)
Feb 2020	Cryptopia	Various	$2.3 million
Mar 2020	BitMEX	Various	N/A
Jul 2020	Twitter	Bitcoin	N/A (social hack)
Oct 2020	KuCoin	Various	$281 million
Dec 2020	Ledger	Various	N/A (data breach)
Apr 2021	hotbit	Various	N/A (ongoing hack)

Current Practices followed by Exchanges

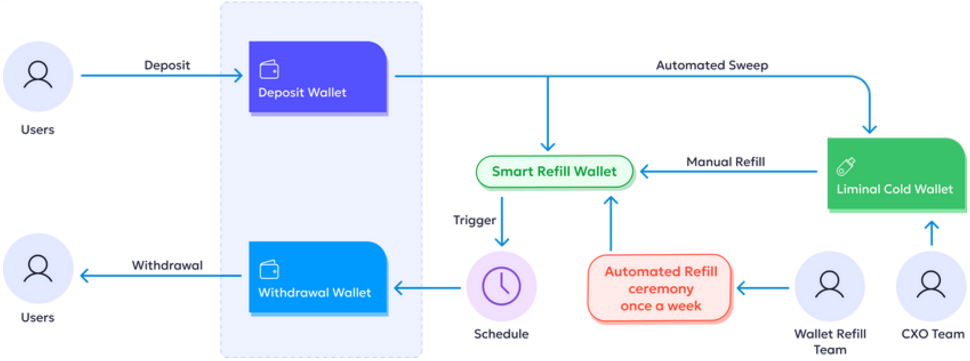
After the early days of crypto exchanges going down, due to loss of their own and investors' assets, standards started to come into place to safeguard their overall security infrastructure from different stand-points.

Starting from very basic activities to using progressive ones, there are certain security practices that every exchange follows in this day-and-age:

- Deploying firewalls, cybersecurity protocols and authentication integration
- Conducting regular code, website and application audits to find and resolve bugs pointing to vulnerabilities,
- Securing major portion of treasury onto a cold wallet using HSMs and
- Implementing advanced wallet technologies like Multi-Signature and MPC for their hot wallets safety and
- Absence of an Insurance coverage to cover the losses and thefts in case of a mishap.

While these security measures formulate a decent strategy to safeguard all exchanges funds, they are still in a nascent stage and do not fully ensure definitive safety of assets or a timely extraction when under a hack.

On the retrospective, there are multiple incidents of top-tier exchanges who had implemented the aforementioned strategies and still got attacked, leading to significant loss of funds, some ceasing to exist, proving how half-prepared today's exchanges are in dealing with security threats.



Current functionality of exchange | Source : Liminal Research

5 Ways Crypto Exchange can safeguard funds

In lieu of how prone crypto exchanges have been and still are to cyber threats, malware, ransomware or factually any kind of vulnerability, it is imperative to opt for improved ways of attaining security across platforms, redeeming their status of, "gateway to crypto".

1. Automation Integration

Crypto exchanges sit right at the center of the cryptocurrency trading ecosystem, churning millions of transactions on a daily basis using a combination of wallets. These transactions mostly happen through the Hot wallet of exchanges, that holds only a sizable amount to carry out the necessary transactions, while the rest of the treasury is generally moved to a cold wallet.

This aspect of wallet management is completely manual-driven, which increases the dependency on resources to do continuous monitoring of wallets, making it error prone.

With automation integrated into their entire wallet infrastructure, exchanges can easily solve the process of to-and-fro from hot wallet to cold wallet, leaving no scope of human-induced error and maintain a standard ratio of funds in hot wallet and cold wallets, reducing risk exposure of hot wallets.

2. Private KeN Management

Out of all the security concerns that loom over digital assets, private key management is the most simple one and yet the most difficult one to perfect as well. With exchanges it becomes an even mammoth task, to safeguard private keys to their hot wallets that hold millions of dollars worth of assets at any time.

The process of private key management is complicated and has to be done with utmost security to make sure that private key access is kept distributed, appointing guardians allocated with permissions to recover in case the private key gets lost or stolen or expires abruptly, enforcing a system to generate keys back and recover wallets.

Hot wallet functionalities have improved exponentially with solutions like Multi-Sig and MPC that only help in assigning more than two entities to take care of both the scenarios of private key management. Both Multi-Sig and MPC wallets once added into an Exchange's hot wallet can ease the way private keys are managed across team members, giving permission to those who are eligible, help recover lost private key with the intimation of 2/3 members only and eradicate potential loss of an entire wallet due to poor private key management.

3. Compliance

Cryptocurrency trading still isn't prevalent in most jurisdictions and modular laws in different geographies. Furthermore, regulations surrounding protecting of user funds, protocol safety standards are more ambiguous than clear.

Working with different organizations, government authorities and consortiums to follow-up on most recent compliance and regulation standards is the best bet for any exchange looking to deploy their services in major geographies and remain operational throughout.

Crypto exchanges can also partner up with industry-leading compliance and regulation certifications to establish an authority over their security infrastructure and further their attempt of safeguarding funds.

4. Custom Workflow

Security and custody measures are different for each protocol and use-case in blockchain but the systems, tools, integrations remain pretty constant in their state of operations and do not extend any extra support to any crypto exchanges.

Every Crypto Exchange has their own analysis, requirement and custom needs based on their scale, operation style, volume processing capability and growth predictions. To comply with all these, crypto exchanges need custom experience to manage their wallets, custody and treasury to keep security at the highest notch and continue expanding.

Custom workflow creation capability into wallet infrastructures can deem-down any unsuspected rise in demands or liquidity crunch on wallets, maintaining the principles of security. In addition to this, creating custom workflows can also reduce redundancies in transaction processing helping to lower down operational inefficiencies. This can help improve the speed and efficiency of transaction monitoring, allowing the exchanges to identify and respond to potential security threats more quickly.

5. Insurance

Lastly it is adamant to think that nothing can go wrong in the world of cryptocurrencies. On the contrary, the notion is quite the opposite. Even after implementing the most stringent of security components, it is possible that exchange can be hit by an untimely hack or theft. At such a moment, insurance coverage can come in real handy to comply with a number of problems.

The first and foremost problem insurance will solve crypto exchanges is sorting our withdrawal request, maintaining continuity in their operation and adhering to the promise made to their investors.

In some jurisdictions, it is essential for a crypto exchange to have cybersecurity insurance before operating. Operating with a sizable insurance protection can help exchanges in elevating their reputation even after going through a security breach and can demonstrate how dedicated they are to protecting their user funds.

What does the future look like for Exchanges?

The actualisation of how crucial it is to hold major part of one's custody, exchanges will have to evolve swiftly, incorporating an array of frameworks with the modus operandi of highlighting transaction security, key encryption, wallet procurement, updated compliance support and risk management of highest sorts.

Exchanges will have to start deploying dedicated systems, workforce, resources to ensure a decentralized directive of financial operation sanctioned through self-custody guidelines. Those who fail to adhere under this methodology will eventually stumble down to losing user trust, liquidity infusion and collaboration opportunities.

Even for those who currently have set up an elongated network of securitising their processes, will now have to focus on improving efficiency quotient making their operational functionality innovative and coherent. Working on this exclusively will only take so much time and to speed it up and settle a competitive edge, exchanges will partner-up with platforms offering Custody-As-A-Service and Wallet-As-A-Service to augment their application into a fathomable reality.

How can automation in hot wallet infrastructure help solve this problem?

The straightforward method to further enhance the safety of assets across any crypto platform's wallet infrastructure is by implementing advanced security features while reducing human involvement to a bare minimum. This goal can be achieved to a great extent by automating the hot wallet refill process. However, such automation solutions should also enable platforms to maintain complete control over the system at all times, allowing for manual interventions and changes in parameters as and when needed.

The need for the hour is an automated, secure hot wallet management solution that doesn't compromise on the platform's autonomy. Liminal has answered the call for such a solution with the Smart Refill.

How does Liminal Smart Refill help?

The highly customizable Liminal Smart Refill solution for hot wallet management supports ready integration into a platform's existing wallet infrastructure. Liminal's Smart Refill Wallet takes the place of a warm wallet to constantly monitor and conduct periodic refills according to parameters set by the platform's refill policies.

Advantages of using Liminal Smart Refill Solution for the platforms include:

- ### Enhanced Security

  The Liminal Smart Refill solution makes use of multisig Smart Refill Wallets enabling the platforms to assign transaction signing credentials to multiple people to ensure redundancy of operations. The involvement of multiple people in authorizing transactions enhances accountability, eliminates single points of failure arising due to compromised private keys, and ensures continuity of operations even in the absence of one or more key holders.

  The transaction signing process is carried out in batches known as Refill Ceremony. The authorized signatories can pre-sign refill transactions with their HSM-enabled devices in advance at their convenience. The compulsory use of hardware wallets for signing provides additional security, while the Refill Ceremony reduces the possibility of all the associated keys simultaneously getting exposed at any given time. Meanwhile, the Smart Refill Wallet retains one signature to be used to complete the signing process only at the time of refill.

  Further, each Smart Refill Wallet is exclusively paired to one hot wallet through a whitelisting process. It effectively eliminates the possibility of fund transfers to any other wallet apart from the one confirmed to be owned and operated by the platform.

- ## Seamless, Uninterrupted Refill Process

The Smart Refill Wallets operate based on the refill parameters specified in advance by the platform. Whenever the conditions in terms of refill frequency or minimum wallet liquidity threshold value match the declared parameters, the Smart Refill process will be initiated automatically.

Using intelligent algorithms, the Smart Refill Wallet guarantees ontime refill transaction confirmation by setting optimal gas fees and initiating follow-up attempts whenever necessary. It keeps the wallet management team constantly updated with alerts regarding the hot wallet status and actions initiated by the Liminal Smart Refill solution. If the hot wallet balance were to fall below the threshold while the Smart Refill Wallet is in the middle of a cooldown phase, the system would alert the team to initiate a one-time manual override to initiate a forced refill.

- ## Flexibility and Control

The Liminal Smart Refill solution is a Plug-and-Play solution that requires minimal changes to existing wallet infrastructure and operational workflow. As a highly customizable solution, it allows the platforms to set refill parameters in accordance with their refill policy. The refill settings, once in place, can be updated at any time by the administrator after completing certain security verification steps.

The manual override option ensures that the operator is always in control of the automated wallet refill solution as well as the funds handled by the Smart Refill Wallet.

- ## Efficient Use of Resources

Apart from reducing the manpower requirements for hot wallet refills using Smart Refill Wallets, Liminal also encourages efficient utilization of funds by the platform. The Smart Refill Wallets don’t require the entire liquidity matching the value of pre-signed transactions to be locked on the platform. Instead, platforms can ensure the availability of sufficient liquidity to satisfy immediate refill needs and put the rest of EVM-based assets to other uses.

Alternatively, platforms can also choose to divert a portion of the funds received in their deposit wallets to fund the Smart Refill Wallet instead of accessing cold wallets for liquidity. Such a practice will introduce some sort of predictability in terms of funds availability, reduce the number of transactions from cold wallets and help in decision-making processes.

Make Your Operations Stress-Free

The Liminal Smart Wallet Refill solution provides a safer and more efficient automation solution for crypto platforms to improve their operations. By minimizing manual intervention in the wallet refill process and implementing additional layers of security without many changes to the existing infrastructure. With Liminal's solution in place, they can carry on with their business as usual while pocketing some extra change in the form of savings

Streamlining Wallet Security and Asset Custody Solution For Exchanges

Liminal is a robust wallet infrastructure and custody platform instilling new definition of secure custody management of digital assets for crypto-native protocols and crypto-progressive institutions.

Liminal is pioneering the innovations in wallet architecture by building a middleware solution to push the boundaries of creating high operational workflows, automate transaction processing and bundling, standardize industry-grade compliance and security norms, metric-driven dashboard view for asset management and more.

- **Enhanced Security**

  The Liminal Smart Refill solution makes use of multisig Smart Refill Wallets enabling the platforms to assign transaction signing credentials to multiple people to ensure redundancy of operations. The involvement of multiple people in authorizing transactions enhances accountability, eliminates single points of failure arising due to compromised private keys, and ensures continuity of operations even in the absence of one or more key holders.

- **Leading Innovation and Excellence**

  At Liminal, we are bringing innovation into the entire process of digital asset management from automation to cost optimisation and to custom workflows for specific business needs.

- **Industry Standard Licensed and Compliant**

  At Liminal, we are strong advocates of regulations and compliance based operations. Hence, we poses some of the most exclusive licenses and continuously applying for more to serve our clients aptly.

- **Procuring Best In-Class Security Elements**

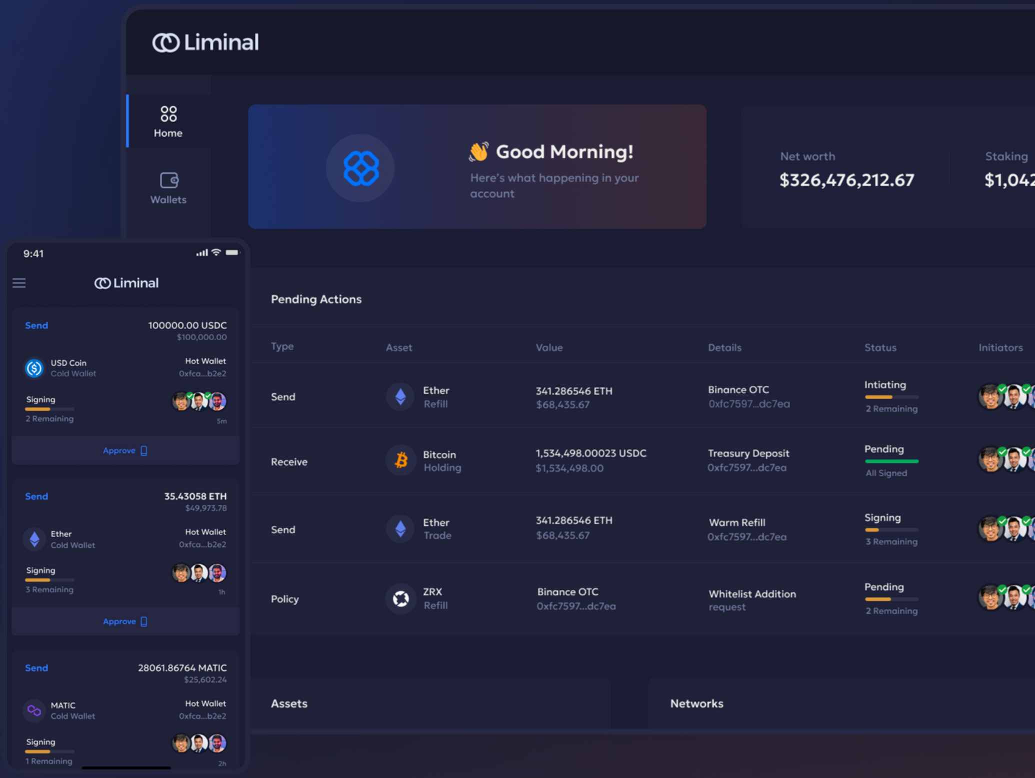
  At Liminal, we have fabricated extremely secure wallet infrastructure and custody protocols with our custom-build applications to aid enterprises in keeping their assets safe and secure.

- **A Mobile First Wallet Approach**

  At Liminal, we always prioritise mobility and through our mobile application we are easing the process of managing and creating MPC wallets, signing transactions, keeping track of assets and more.

Liminal

Follow Us For More Updates On The Groundbreaking Innovation We Put Into Our Wallet Infrastructure and Custody Platform



👋 Good Morning!

Here's what happening in your account

Net worth
$326,476,212.67

Staking
$1,042

Pending Actions

Type	Asset	Value	Details	Status	Initiators
Send	Ether Refill	341.286546 ETH $68,435.67	Binance OTC 0xfc7597...dc7ea	Intiating 2 Remaining	
Receive	Bitcoin Holding	1,534,498.00023 USDC $1,534,498.00	Treasury Deposit 0xfc7597...dc7ea	Pending All Signed	
Send	Ether Trade	341.286546 ETH $68,435.67	Warm Refill 0xfc7597...dc7ea	Signing 3 Remaining	
Policy	ZRX Refill	Binance OTC 0xfc7597...dc7ea	Whitelist Addition request	Pending 2 Remaining	

Assets

Networks

Send
100000.00 USDC
$100,000.00
USD Coin
Cold Wallet
Hot Wallet
0xfca...b2e2
Signing
2 Remaining
5m
Approve

Send
35.43058 ETH
$49,973.78
Ether
Cold Wallet
Hot Wallet
0xfca...b2e2
Signing
3 Remaining
1h
Approve

Send
28061.86764 MATIC
$25,602.24
MATIC
Cold Wallet
Hot Wallet
0xfca...b2e2
Signing
1 Remaining
2h

$550 Mn+
Assets under protection

$600 Mn+
Wallet refills processed

$6000 Mn+
Transactions processed

1000 +
Manual hours saved

CCSS
Qualified Service Provider
Cert ID: CCSS00001 Issued by C4

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

PS
ISO/IEC 27001:2013 CERTIFIED by
PRESCIENT SECURITY
verify

www.liminalcustody.com