

WHITE PAPER

Fireblocks' Multi-layer Philosophy for Securing Digital Assets



Table of Contents

04	The attack vectors
10	What makes a multi-layer solution?
11	The previous generation of digital asset security
15	The next generation of digital asset security
19	The Fireblocks multi-layer security solution
24	Protecting digital assets in 2021
25	About Fireblocks

Fireblocks' Multi-layer Philosophy for Securing Digital Assets

Digital assets are vulnerable to hacking throughout their entire lifecycle, and cybercriminals take advantage of these vulnerabilities every step of the way. In fact, hackers have stolen **over \$15 billion total in crypto in the past 8 years**.

With 20+ years of industry experience among each of our leaders and an academic cryptography advisement team, we understand that no security technology alone is unbreakable. As we've seen over the years, the best defense against cybercriminals is a multilayered one that can provide redundancy in the event that one of the security controls fails.

That's why, at Fireblocks, we've designed a security system that layers the strongest software and hardware defenses to make breaking in highly expensive and nearly impossible – creating a truly secure environment for storing, transferring, and issuing digital assets.

At the same time, Fireblocks is designed to support the operational needs of a digital asset business. We mitigate the top threats to digital assets, while delivering the necessary speed, flexibility, and tools to meet your business objectives.

In this white paper, we'll walk you through everything you need to know about protecting digital assets.

WHAT IS MULTI-LAYER SECURITY?

Multi-layer security is an approach to cybersecurity in which multiple defensive mechanisms are deployed in tandem to protect data and information. A methodology of this sort – in which one layer of security being compromised doesn't break the entire system – is able to address a variety of attack vectors at once and decrease the likelihood of a successful breach.

In cybersecurity, experts often refer to this type of security as the "castle approach" due to its structural similarity to a medieval castle. To penetrate a castle, attackers must get through several layers of security, namely the moat, ramparts, drawbridge, towers, battlements, etc.

The Attack vectors

In order to fully protect your digital assets, it's first important to understand how cybercriminals usually compromise them. If your solution accounts for the 3 primary attack vectors that hackers focus on, you can fully secure your asset storage and transfer process. These attack vectors include:

- ▲ Private keys
- ▲ Deposit addresses
- ▲ Credentials and authentication

Private Keys

Hackers and other malicious actors (such as rogue employees) may attempt to compromise a victim's private keys in order to access their wallet, which controls the funds they have stored on the blockchain. This enables the attacker to transfer the funds from the victim's wallet to anywhere – i.e. into their own wallet. One example of this is the [Cryptopia hack of January 2019](#), in which professional hackers stole \$16 million by compromising Cryptopia's wallet system. Some of the ways in which private keys have been compromised before include:

- ▲ Infecting a server with malware that steals the private key.
- ▲ Stealing an HSM (hardware security module) authentication token and forcing the HSM to sign a withdrawal transaction.
- ▲ An authorized internal employee steals the private key.

Today, institutions in the digital asset space are securing private keys using MPC (multi-party computation). MPC represents a powerful next step in private key security because it removes the single point of compromise, and it's even more effective if it's secured in hardware.

Some digital asset security solutions stop at MPC because it's a great technology for securing private keys. But if your institution is looking to actually move and transfer digital assets on a consistent basis (which is necessary to build a profitable business model in the space), it's important to also secure deposit addresses.

3I1xwTTaCwLkMk2a6cbD8K4W1HPfKfQj0k

12DLEmbmkeyfD7qLa9Xm3BYKc7FWcYSu0

3JeME8GeAY5wte9TdJAuZZMeDYU1Kcd8LU

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNUN2

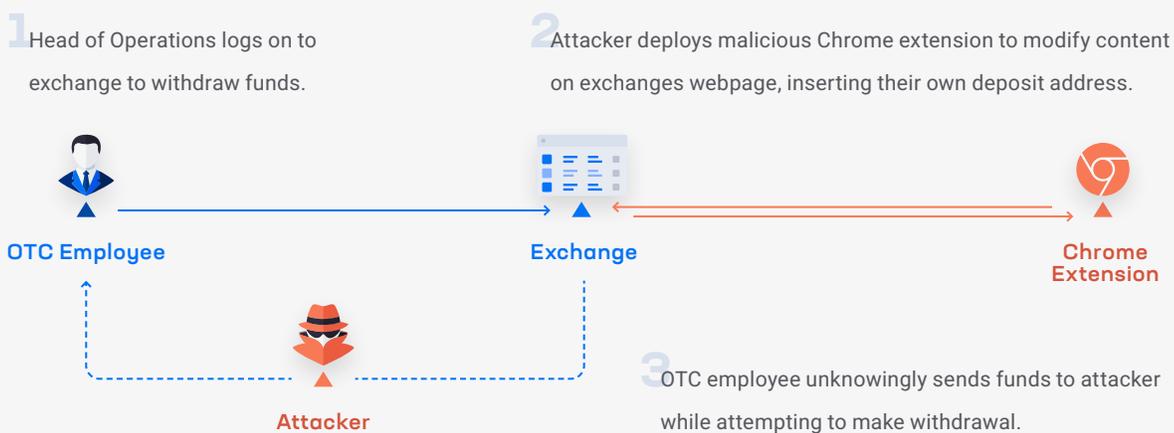
But it's important to understand that private keys aren't the end of digital asset security. For institutions that only need to secure digital assets in storage and don't need to instantly access or move their assets, focusing on private keys is adequate. However, if the assets are being transferred between trading venues, liquidity providers, customer accounts, and other counterparties, it's necessary to also secure deposit addresses and API credentials.

This is one of the reasons why some digital asset security solutions stop at MPC – because it's a great technology for securing private keys. But if your institution is looking to actually move and transfer digital assets on a consistent basis (which is necessary to build a profitable business model in the space), it's important to also secure deposit addresses.

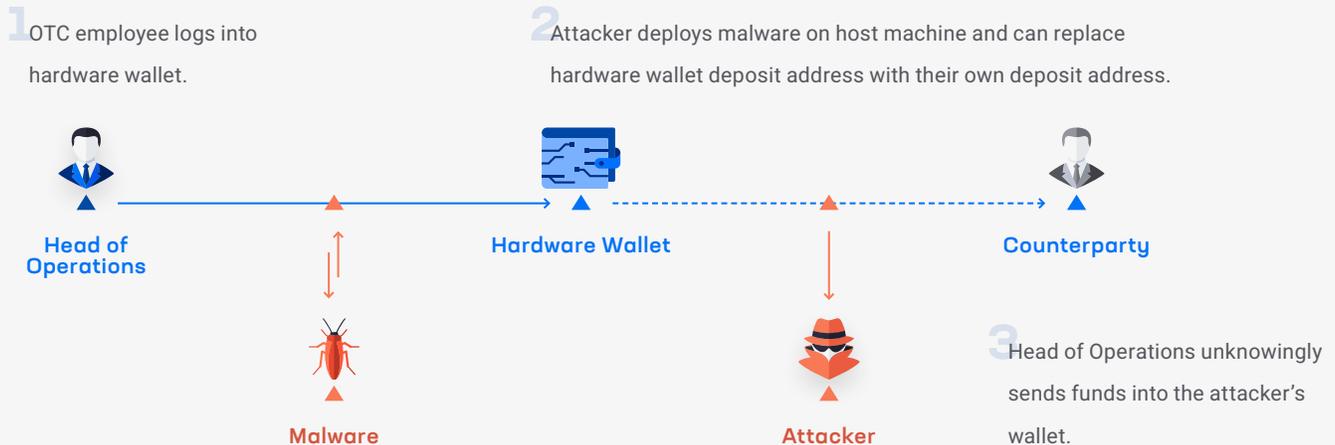
Deposit Addresses

A deposit address is a long alphanumeric string that designates the public address of a wallet. To transfer funds to a counterparty, it's necessary for both parties to exchange deposit addresses. Hackers **target the deposit address exchange process at a number of points along the way**. Here are a few common attacks:

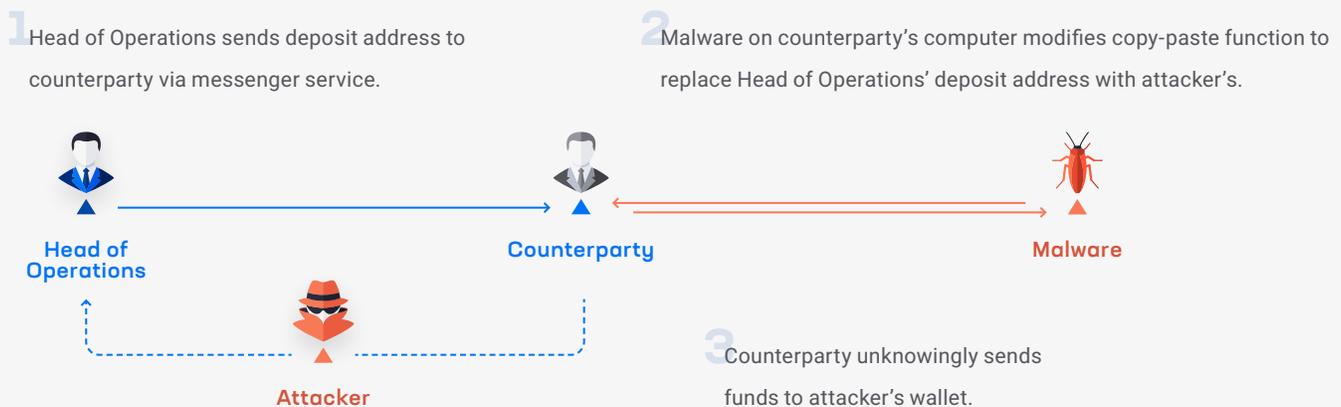
Fraudulent Chrome web extensions that hijack the web browser (man-in-the-browser).



Malware on a counterparty's computer that modifies the copy 'n' paste of a deposit address to send assets to the hacker's wallet



Malware that hijacks the wallet interface.



OTHER WAYS HACKERS COMPROMISE DEPOSIT ADDRESSES

- ▲ Spoofing the address while copy and pasting between the web browser and the wallet's app.
- ▲ Intercepting and modifying the deposit address while it's being sent between counterparties on a messaging service (i.e. Telegram).
- ▲ Hijacking code on the exchange's website to spoof the address at the origin – such as the gate.io exchange hack that relied on a code breach of the web service StatCounter.

In one prominent attack, hackers stole \$140,000 in BTC through a man-in-the-middle attack that morphed copied & pasted deposit addresses into ones of the hackers' choosing.

A number of methods have been utilized to mitigate the threat of deposit address compromise. Some of the most common methods for securing deposit addresses include test transfers, whitelisting, and hardware wallets. Though these security measures have their benefits, there are also certain issues with them that should be considered:

- ▲ Test transfers are meant to ensure that the deposit address has not been compromised in transit—which could occur by hackers intercepting and modifying the deposit address, and ultimately sending assets to their own wallet. Though this manual security protocol adds another layer of safety, test transfers can be very time-consuming and far from foolproof.
- ▲ Whitelisting asks a number of professionals within an organization to devote time to a manual procedure. While it can be a powerful security measure, whitelisting ultimately cannot prevent internal fraud, as a rogue employee can go into the organization's spreadsheet or database and swap out the deposit address of a certain whitelisted counterparty for their own. In addition, whitelisting cannot stop human errors (such as a simple fat-fingers error entering a deposit address into the whitelist, or a counterparty rotating a deposit address without the correct re-entry procedure).
- ▲ With hardware wallets, the deposit address is displayed on a hardware device with a small screen. Unfortunately, if your computer has been compromised, the deposit address that is presented on the hardware device will be fraudulent. The assumption being made with hardware wallets is that it's impossible to compromise the hardware wallet because of its hardware isolation. However, hardware wallets cannot prevent interference with the user's computer.

Credentials and Authentication

One of the most common methods hackers use to compromise digital assets is impersonating a user within an organization. As the digital asset ecosystem is interconnected, the hackers can utilize the credentials and authentication of the user to either compromise wallets in custody or accounts on exchanges and

liquidity providers. Once the hackers are able to login, they can issue and authorize fraudulent transfers.

- 1 The oldest form of attack is achieved by compromising the username and password (credentials) of an organization's users and logging into that organization's services on their behalf.
- 2 In addition many services require two-factor authentication (2FA). This is designed to protect against a compromise of user credentials. Unfortunately, many services allow 2FA using SMS, which is susceptible to SIM swaps – and in extreme cases, [hackers are able to deploy attacks that can defeat one-time password \(OTP\) generators](#).
- 3 Exchanges and liquidity providers often have users utilize API keys for automated access to their platforms. These keys are vulnerable to traditional forms of malware. API keys stored in trading software can also be stolen if the server or code repository is compromised. In general, once a hacker obtains API keys, it's possible for them to instruct unauthorized withdrawal of funds from an exchange or manipulate the market using pre-funded assets on a compromised account.

One of the most prominent examples of an attack based on compromised API keys was the Binance exchange hack (May 2019). Hackers used phishing and viruses to obtain a large number of API keys. They made off with 7,074 BTC – worth more than \$40 million on the day of the attack – in just one transaction.

Today, institutions use chip-level hardware isolation and biometric factors to securely authenticate users and store API secrets. The unique security properties of chip-level hardware enclaves guarantee confidentiality and execution integrity. In addition, Android and iPhones include hardware-isolated biometric authentication capabilities. This prevents hackers and hosting providers from accessing credentials/keys and enables a strong multi-factor authentication of users that is not susceptible to spoofing.

What makes a multi-layer solution?

In the digital asset industry, the definition of and requirements for a true multi-layer solution has evolved over the years. The following threats – and the security layers deployed in response to them – are key to any solution:

Threat Vector	Defense Layer	
Private key compromise	Threshold signatures (e.g. MPC)	Distribution of the private-key into shares using a threshold signature across several servers or devices such that the whole private key cannot be extracted from a single device if a hacker or insider compromises the device
Rogue admin (or hacker that was able to compromise an administrative account) takes control of all machines holding private key shares	Hardware isolation	Protection of each individual key share using hardware isolation, such that even if an attacker controls the machine they cannot extract any individual private key share
Physical attack which steals or destroys all the devices	Physical distribution	Distribution of devices across several physical data centers
Man-in-the-middle or human error on deposit addresses	Verification of deposit address	Attestation of the deposit address of counterparties using secure channels that are immune to both network and host-based man-in-the-middle attacks
Internal employee collusion	Workflow and policy	Separation of duties across multiple organizational functions and enforcement of policies/approval workflows

The previous generation of digital asset security

In this section, we'll walk you through the previous generation of security technologies that were utilized to protect digital assets. These technologies were widely utilized in earlier attempts at protecting digital assets. However, they are no longer able to support the operational and security needs of today's digital asset businesses, and they provided the foundation upon which today's next-generation systems were built.

Multisig

Multisig (multi-signature) is a digital signing process that enables two or more users to sign transactions as a group. Before multisig wallets entered the mainstream, cryptocurrencies were generally stored using a single private key. Whoever had access to the private key itself was able to access the funds associated with that key. Multisig added an additional layer of security to the equation by creating wallets that require the signature from multiple keys.

While multisig offers potential solutions to some of the problems of single-signature wallets (e.g. the single point of failure), it also introduces new issues. This is because when multisig was first introduced in 2012, the blockchain space was different in a variety of ways. For example, bitcoin was the only cryptocurrency, so the concept of creating a security technology that would work across multiple blockchains was irrelevant. In today's digital asset landscape, multisig-based solutions are outdated for the following reasons:

MULTISIG IS NOT PROTOCOL AGNOSTIC

Not all cryptocurrency protocols support multisig – and those who do have very different implementations from one another. This makes it more difficult for multisig wallet providers to support new chains.

With an on-chain multisig solution, each protocol requires the wallet provider to implement a different code. When a multisig implementation goes wrong, various issues can arise:

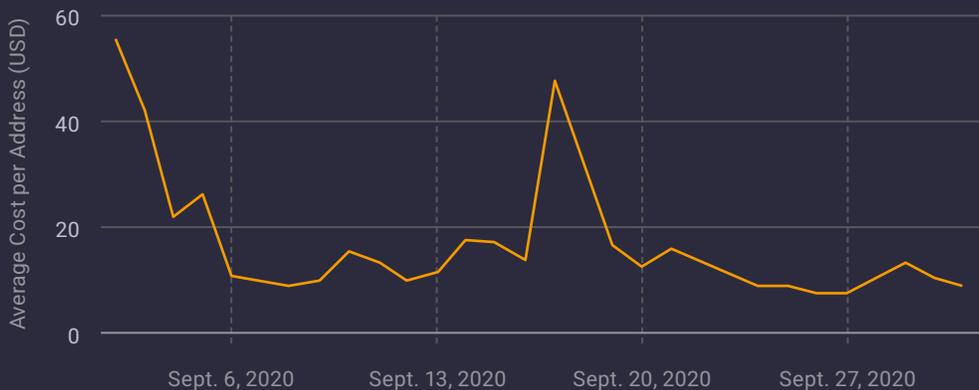
- ▲ **The Multi-Sig Parity Wallet** - Poor implementation lead malicious actors to steal around \$30m worth of Ethereum in one of the biggest wallet hacks to date.
- ▲ **Parity Wallet Hacked (Again)** - A hacker again gained access to the wallet and froze \$300m worth of Ethereum. Some customers lost up to \$300k worth of digital assets.
- ▲ **Vulnerabilities in Bitcoin Multisig** - Discovered by the Fireblocks Research team, a vulnerability in the bitcoin multisig check implementation was deployed in development environments and, despite the popularity of this codebase, the vulnerability still remains.

MULTISIG IS OPERATIONALLY INFLEXIBLE

Multisig cannot offer the operational flexibility organizations require as they grow.

As your team expands, you will need to adjust the process of accessing and transferring your digital assets. This can include changing the number of employees required to sign a transaction, adding new key shares as you hire new employees, revoking key shares as employees leave, and modifying the required threshold to sign transactions (e.g. from '3 of 4' to '4 of 8'). In these sorts of scenarios, multisig addresses create various obstacles, as they are pre-set to the wallet.

Ethereum Multi-Sig Address Generation Cost



Multi-sig is not protocol agnostic; on the Ethereum protocol, address generations can get extremely expensive when compared to other solutions (such as MPC).

HSM (Hardware Security Module)

A hardware security module (HSM) is a physical device – separate from a computer – that provides extra security for sensitive data. Businesses may use an HSM to secure cryptographic keys by ensuring only authorized individuals can access the HSM.

While HSMs do introduce a powerful layer of security, they are vulnerable to internal attackers when they are utilized alone. If an entire private key is stored on an HSM and multiple parties within an organization have access to it, there's nothing to stop a rogue employee from signing a fraudulent transaction using a private key stored within it.

As HSMs have a fairly limited logic, the request to sign a transaction is validated against an external access token that a server or computer store. Any user, or a hacker that compromised their computer, can obtain the authorization token and force the HSM to sign a transaction that will withdraw the entire amount from the wallet.

Due to their limited resources, HSMs cannot protect critical policies or workflow logics, forcing wallet providers that use HSMs to implement such logic in user-mode. This type of setup exposes the wallet to both external hackers and insiders that can easily modify the whitelisting and velocity withdrawal policies. This occurred in the famous **BitGo-Bitfinex hack**, where some blamed BitGo HSMs for “blindly signing” the withdrawal of nearly 120,000 BTC after the policy was changed by the hackers.

Moreover, the limited resources of HSMs prevent them from running next-generation cryptography – such as MPC and zero-knowledge algorithms.

In addition, HSMs pose various operational problems. In today’s remote-forward work environments, the necessity to have certain employees physically present wherever the HSM itself is located can be a serious issue. And if your organization is transferring digital assets with any consistency, you don’t want to be dealing with the added inconvenience of moving data (such as private keys) in and out of an HSM.

FIREBLOCKS BRINGS YOU

The next generation of digital asset security

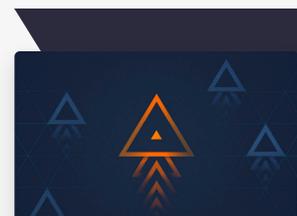
MPC (Multi-Party Computation)

MPC (multi-party computation) is the next generation of private key security.

MPC is a cryptographic technology that allows multiple parties to each hold secret information and then solve a problem that requires the input of all these secrets in a decentralized way, without ever sharing the secret information with one another.

Fireblocks developed the **MPC-CMP protocol** that applies this concept to blockchain-based ECDSA and EdDSA signatures (used by all blockchains). MPC-CMP removes the concept of a single private key; such a key is **never gathered as a whole, neither during the first creation of the wallet nor during the actual signature**. MPC-CMP follows a set of steps to guarantee that there is never a single point of compromise of the private key:

- 1 Individual secrets are randomized by each of the several (always more than 3) endpoints – either servers or mobile devices. Those secrets are never shared with each other.
- 2 The individual endpoints engage in a decentralized wallet creation protocol in which they compute the public key (wallet address) that corresponds to the set of individual private shares.
- 3 When a signature on a blockchain transaction is requested, a quorum (at least 3) of endpoints engage in a distributed signature process where each one of the endpoints individually validates the transaction and policy and signs the transaction.



Pushing MPC Wallet
Signing Speeds 8X
with MPC-CMP

MPC-CMP: A New Breakthrough in MPC Technology

	FIREBLOCKS MPC-CMP WALLET	GENERAL MPC WALLET
Single point of private-key compromise	NO Secure MPC	NO Secure MPC
Hardware based isolation	YES All shares are chip-level isolated	NO
Cryptographic authentication for signature access	YES Passcode + bio / Yubikey	NO
Secure Transfer Environment for institutional transfer and E2E authentication of deposit addresses with counterparties	YES All shares are chip-level isolated	NO
Deployment Options	PaaS, SaaS	SDK, PaaS

In a similar fashion to multi-sig, the MPC-CMP private key protection layer removes the single point of compromise from both external hackers and insiders – as the private key is never concentrated on a single device at any point in time.

At the same time, MPC’s distributed nature allows team members to require multiple authorizers for a transaction and sign transactions without being in the same location. Operationally, it’s a significant advancement over multisig due to its inherent flexibility; unlike multisig, MPC allows for ongoing modification and maintenance of the signature scheme. To use the example detailed above, changing from a ‘3 of 4’ set-up to any other set-up would simply require existing shareholders to agree on the new distributed computation and the addition of a new user share. **In this process the blockchain wallet address (deposit address) is maintained, so that you don’t need to create a new wallet, move any funds, or provide counterparties with a new address.**

MPC-CMP was designed to address new requirements of the digital asset space that have emerged as institutions have entered the ecosystem – and it's designed to be future-proof.

MPC-CMP offers:

- ▲ Multi-blockchain support
- ▲ Institutional user base with the ability to add and remove users to the quorum
- ▲ Lowest fees for blockchain transactions as the # of transactions increases 2X every 2 years
- ▲ Compatibility with cold storage
- ▲ Universal composability
- ▲ 1 transaction round (6 to 9 rounds in all other MPC protocols)
- ▲ Automatic key refresh
- ▲ Open-source and peer-reviewed

Intel SGX (Software Guard Extension)

Intel SGX is a hardware-level enclave that isolates selected code and data within a system, similar to an HSM from the operating system. It is designed to protect the cryptographic material, the cryptographic algorithm, and the execution of sensitive parts of the software from both insiders (such as rogue admins) and hackers. Compared to an HSM, SGX offers a variety of benefits, including:

- ▲ The ability to protect next-generation cryptographic algorithms such as MPC and zero-knowledge proofs
- ▲ The ability to isolate and protect policy engines, whitelisting databases, and workflows from insiders and hackers
- ▲ Strong, hardware isolated authentication of users by end-to-end attestation of secure-enclaves (ARM TrustZone) in mobile devices and hardware tokens (such as Yubikey)
- ▲ High degree of scalability across public clouds and on-prem deployments, increasing security, availability, and redundancy

In general, SGX offers a great deal of operational elasticity while providing the security associated with a traditional HSM. For digital asset businesses that require the highest level of hardware-based security in tandem with speed and flexibility, SGX is a very strong option.

The Fireblocks multi-layer security solution

The Fireblocks R&D team created a multi-layer security matrix that layers MPC, Intel SGX, our signature Policy Engine, and a deposit address authentication network to build the most impenetrable system on the market. This ensures that our customers' assets are protected from cyberattacks, internal colluders, and human errors.

Layer 1: MPC + Multi-Cloud

We selected MPC over multisig to remove the single point of compromise from sensitive pieces of data (such as our users' private keys) for several reasons:

- ▲ **Operational flexibility.** It's important to us that our solution can stay on pace with our users' needs as their organizations grow, and multisig simply doesn't allow that.
- ▲ **Unbiased.** MPC is the only key-sharing technology available that works across all blockchains.
- ▲ **Cheap.** Wallets based on multisig are associated with higher fees than regular, single address transactions. MPC-based wallets, however, are represented on the blockchain as a single wallet address, with the actual distributed signature computed outside of the blockchain. This means having the lowest fees possible for each transaction.
- ▲ **Fast.** MPC-CMP pushes MPC transactions speeds up to 8X faster than ever before.

Fireblocks offers users multiple options for distributing the cryptographic MPC shares to ensure an extra layer of security even if one of the physical datacenters is compromised:

- ▲ Distribution across multiple tier-1 cloud providers (Microsoft Azure and IBM Cloud)
- ▲ Distribution across several on-prem datacenters
- ▲ Hybrid (on-prem datacenters and cloud providers (such as Microsoft Azure) are used simultaneously)

Layer 2: SGX

For the hardware layer of our security solution, we selected SGX over a traditional HSM. Using SGX enclaves on a minimum of 3 to 5 machines (each of which on a segregated network), we distribute private keys with an extremely high level of security.

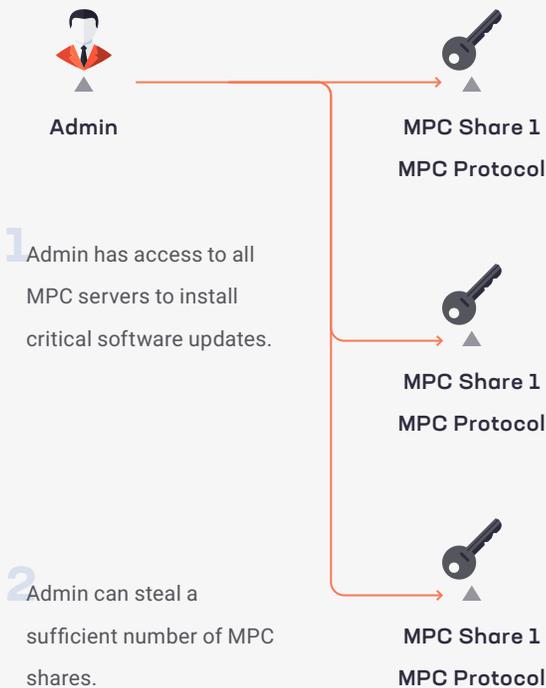
USING MPC FOR API KEYS & CREDENTIALS

Unlike multisig, MPC can also be applied to API keys and credentials. Fireblocks recently developed HMAC-MPC, an algorithm which uses MPC to remove the single point of compromise from API credentials. The Fireblocks HMAC-MPC algorithm also enables storing the API key shares within an HSM-like environment, sealed using a hardware key.

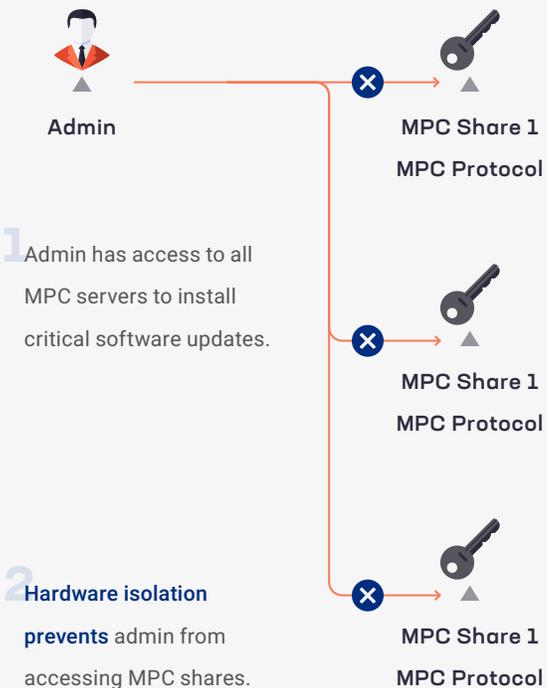
As the keys are stored in SGX, they cannot be extracted even if malware or a hacker has control over the server's OS – as the memory space and the data in the SGX enclave are encrypted.

We also utilize SGX to secure API keys. In the trusted execution environments (TEEs) in which we store these exchange credentials, the information cannot be retrieved by hackers, inside colluders, or even Fireblocks employees.

USER-MODE MPC



FIREBLOCKS HARDWARE ISOLATED MPC



Layer 3: Policy Engine

The Fireblocks Policy Engine, which enables organizations to set up specific approval policies for every transaction, represents the next step for digital asset security.

The Policy Engine allows users to configure a list of rules that affect how transactions are handled and approved. A rule can set whether a transaction is blocked, approved, or requires additional signers using filters such as source, destination, asset, and amount.

Here are some examples of possible rules that could be applied to an organization using the Policy Engine:

- ▲ When one of the traders in the team makes a transfer to external wallets, it will require a second approval by one of the other team members.
- ▲ Any transfer to an external wallet above \$50k requires an approval by either the Ops team leader or two members of the Ops team.
- ▲ Block all transfers from the vault to any wallet or exchange if the total volume has exceeded \$100M in the last 24 hours.

Fireblocks secures the Policy Engine itself using SGX and distributes policy verification across several MPC servers. Policy rules are signed by a quorum of admins and encrypted within SGX; the engine is implemented inside of the SGX enclave and the code cannot be modified. This prevents both hackers and even insiders (such as IT administrators) from modifying the implemented rules or the logic of the policy engine.

Settlement Layer: The Fireblocks Network

The settlement layer of our multi-layer system is the Fireblocks Network, an institutional asset transfer network that completely mitigates the risks associated with deposit addresses by automating deposit address authentication and rotation.

The Fireblocks Network entirely removes the need for copy-pasting deposit addresses and then authenticating them using time-consuming and risky test transfers and whitelisting procedures. Without an authentication network, it's possible for assets to be lost through deposit address spoofing or human errors (such as entering a deposit address for a counterparty that they've already rotated out).

Institutions on the Fireblocks Network settle trades within seconds, and don't have to worry about the possibility of asset loss due to a deposit address attack or error.

The Fireblocks Network is built using a patent-pending technology that is using the latest breakthroughs in secure enclave technology and data-in-motion encryption. The sending wallet opens an encrypted tunnel with the recipient wallet to query for the deposit address to send the transaction to. The encrypted tunnel is protected within a secure enclave (hardware termination) on both the sending wallet and receiving wallet. This guarantees the following security capabilities:

- ▲ Full mitigation of man-in-the-middle attacks on both the network and host levels
- ▲ Proofing the the address at the source, and full authentication of the recipient
- ▲ Guaranteed fail-close system if an attack is detected on either end
- ▲ Automatic rotation of deposit addresses on every transfer to preserve pseudo-anonymity

Protecting digital assets in 2021

In today's digital asset landscape, security is absolutely paramount; in fact, with global crises like the coronavirus pandemic, **cybercrime is only ramping up**. So, how exactly should you go about securing your digital assets in 2021?

By securing your private keys, deposit addresses, and credentials, you can mitigate cyberattacks from both inside and outside the organization.

Until now, this meant utilizing technologies like multisig, or HSMs. Many custody providers relied on one of these technologies in isolation (or even a newer technology, like first-gen MPC) to safeguard assets.

However, in today's market, these technologies are not sufficient enough to both withstand attacks and support evolving business operations. In order to turn a profit with digital assets, operational flexibility and efficiency are of the utmost importance. Last-gen tech is simply too slow and cumbersome to support today's rapidly changing market – and when it's used in isolation, it's also far too weak to protect assets from today's complex attacks.

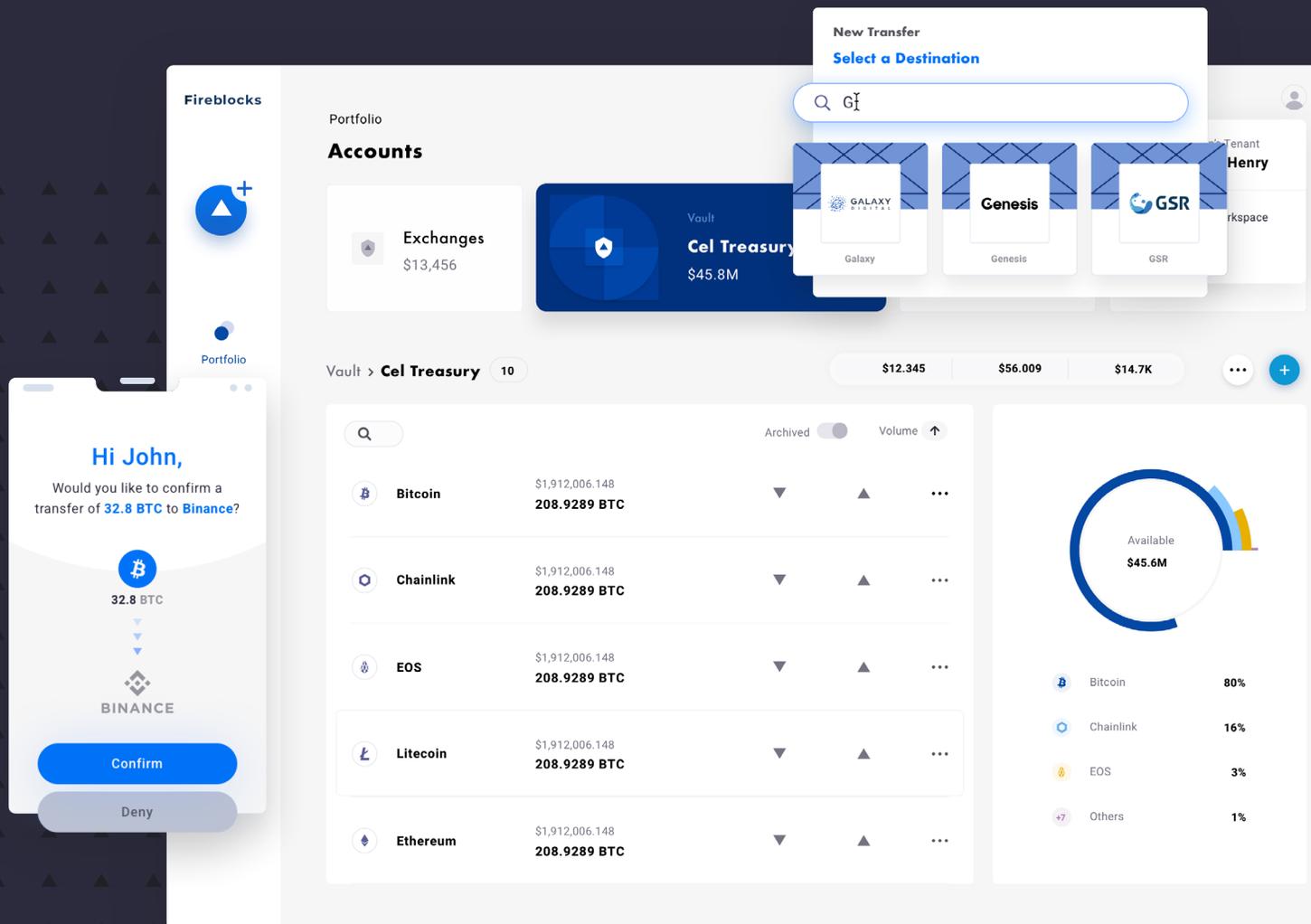
Fireblocks utilizes the latest security technologies – including **MPC-CMP, Intel SGX, Workflow Authorization**, and an **institutional asset transfer network** – in a battle-tested, layered implementation. This is our “multi-layer” security philosophy: by utilizing multiple security controls that aren't reliant on each other, we ensure that your entire business does not rely on one layer of security.

The Fireblocks platform is designed to provide the necessary speed, flexibility, and cost savings to meet business goals while ensuring that every cyberattack vector is completely mitigated.

About Fireblocks

Fireblocks is an enterprise-grade digital asset security platform for moving, storing, and issuing digital assets. Fireblocks enables financial institutions to securely build, run and scale digital asset operations through the Fireblocks Network and MPC-based Wallet Infrastructure. The company has secured the transfer of over \$2.3 trillion in digital assets and offers a unique insurance policy that covers assets in storage & transit.

To see Fireblocks in action reach out to sales@fireblocks.com.
Learn more at [Fireblocks.com](https://fireblocks.com).



The screenshot displays the Fireblocks user interface. On the left, a confirmation modal asks 'Hi John, Would you like to confirm a transfer of 32.8 BTC to Binance?' with 'Confirm' and 'Deny' buttons. The main dashboard shows a 'Portfolio' section with 'Accounts' including 'Exchanges' (\$13,456) and 'Vault' 'Cel Treasury' (\$45.8M). A 'New Transfer' modal is open, showing 'Select a Destination' with options for Galaxy, Genesis, and GSR. Below, the 'Vault > Cel Treasury' view shows a table of assets:

Asset	Value	Balance	Actions
Bitcoin	\$1,912,006.148	208.9289 BTC	▼ ▲ ⋮
Chainlink	\$1,912,006.148	208.9289 BTC	▼ ▲ ⋮
EOS	\$1,912,006.148	208.9289 BTC	▼ ▲ ⋮
Litecoin	\$1,912,006.148	208.9289 BTC	▼ ▲ ⋮
Ethereum	\$1,912,006.148	208.9289 BTC	▼ ▲ ⋮

Summary statistics for the vault: \$12.345, \$56.009, \$14.7K. A donut chart shows 'Available \$45.6M' with a breakdown: Bitcoin (80%), Chainlink (16%), EOS (3%), and Others (1%).