




WHITE PAPER

Digital Asset Wallet Security - A Comparison: Multi-Signature and Multi-Party Computation

Part of BitGo's Security Series for Institutional Investors

Table of Contents

01	Defining Multi-Signature and Multi-Party Computation Protocols	1
02	Overview of Multi-Signature Security	1
03	How Multi-Signature Security Works	2
04	Overview of Multi-Party Computation	3
05	Conclusion	5



01 Defining Multi-Signature and Multi-Party Computation Protocols

It is important to consider all aspects of implementation and security when deciding on a protocol for storing your company's digital assets. In this piece, we take a look at the benefits of multi-signature technology and compare it to multi-party computation as a stand-alone solution to protect digital wallets.

What is Multi-Signature (Multi-Sig)? Multi-Signature is a blockchain security feature which allows two or more users to securely sign documents as a group. In the case of digital assets, funds are stored using a multi-signature address and must be accessed by two or more keys, which are held by separate entities. This enables digital asset holders to create additional policy layers of security for their funds.

What is Multi-Party Computation (MPC)? Multi-party computation is a cryptographic method that has just begun to be applied to digital wallet security. Multi-party computation protocols enable a single key to be split across multiple entities or individuals. With multi-party computation, the key is never combined in one location or on one machine. Multi-party computation uses an iterative process to rebuild a digital signature using mathematical operations that are conducted on separate machines. The resulting signature appears identical to a single signature system.

02 Overview of Multi-Signature Security

BitGo pioneered multi-signature security in 2013 and, since then, it has become an industry standard for security of digital wallets. A multi-signature wallet leverages the blockchain to make use of distinct private keys held by multiple entities. Specific features and benefits of multi-signature include:

Security

Multi-signature, as the name suggests, offers the wallet holder multiple signatures, or keys, in order to eliminate a single point of failure. The most common set-up is 2-of-3, but organizations can also choose 3-of-3, 3-of-4, etc. The main reason for this configuration is to remove a single point of failure because at least two separately managed keys are required to access funds.

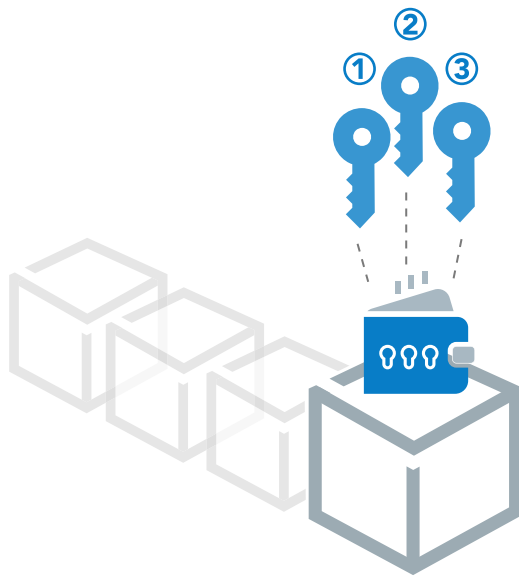
Hardware Security Module (HSM)

An HSM is a physical computing device that secures and manages digital keys adding an additional layer of security to multi-signature protocols. Multi-signature protocols enable the use of HSMs that are purpose-built specifically for cryptographic keys. These single-purpose, air-gapped devices reduce security risks, such as hacks or malware because the keys are decrypted and signed within the HSM. HSMs have been in standard use in banking for years and currently only work with multi-signature security protocols.

Open-Source, Community Tested

Multi-signature is an open-source protocol and is built into blockchain consensus. This allows the developer community the ability to review and test the code. Since BitGo's multi-signature solution has been available since 2013, it has been thoroughly battle-tested, hardened and peer reviewed.

03 How Multi-Signature Security Works



- Multiple keys are created
- Public part of the keys are shared amongst participants and on the blockchain
- Multiple signatures, one from each key, are required for transactions to be valid
- Keys can be in multiple geographic locations and/or held by multiple people
- Blockchain transparency enforces the required number of signatures

Accountability

Accountability is crucial when it comes to digital assets. Similar to fiat transactions, institutions need to be able to set-up and enforce their corporate treasury policies. Additionally, it is critical to know who is signing on any transfer of digital assets.

With multi-signature, there is accountability on-chain. It is explicit which private keys are used to sign a transaction. The blockchain will identify the specific keys - often assigned to an individual or entity - used to transact. This is critical for organizations that require auditability, and must be able to record and trace who has signed a transaction.

Cold Storage

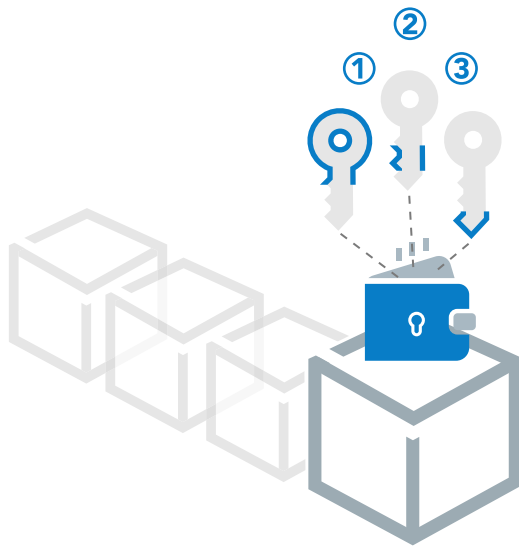
Multi-signature offers the ability to have multiple keys secure an account, some of which may be placed in cold storage. Cold storage, also referred to as cold wallets, are offline wallets for holding digital assets. With cold wallets, the digital wallet is stored on a platform that is not connected to the internet. This protects the wallet from hacks, unauthorized access, and other vulnerabilities. Storing keys offline is not complex, and, with multi-signature, does not require an iterative process which is necessary when using multi-party computation.

Institutional investors adopt multi-sig because they need clear, traceable transactions and enforcement of their corporate treasury policies.

04 Overview of Multi-Party Computation

Multi-party computation is still in early stages as a protocol for holding digital assets. The multi-party computation model relies on a single key; the key can be divided into parts, or shards, and is reassembled iteratively to build a digital signature. This allows for distribution of the parts or shards geographically and/or over multiple personnel or entities. The resulting signature after the multi-party computation operations appears identical to a single signature system.

As an institution looking to safeguard digital assets, it is important to understand how using multi-party computation as a stand-alone protocol affects the security of your digital assets.



- One key divided into multiple shards
- A single key is never reassembled at one location
- Multiple machines used iteratively to build digital signature
- This allows for distribution geographically and over multiple physical personnel or entities
- Resulting signature after MPC operations appears identical to a single signature system

Security

Multi-party computation technology assembles security keys mathematically from separate machines. It thus eliminates a single point of failure by not bringing the keys together on the same machine to enact a signature.

Support For Single-Signature Digital Assets

Not all digital assets support multi-signature protocols. There are digital assets with blockchains that only allow for single signature security. As of this writing, those assets must be supported by multi-party computation or smart contracts. Multi-signature does not have the ability to support single-signature digital assets at this time.

Proprietary Code

The implementations of multi-party computation for the cryptocurrency space that are currently live are largely proprietary. This means that there is no open review of code, recovery tools, operational procedures (e.g. SOC2 audits), etc. Without client and/or community review, there is no way to ensure the safety of funds without trusting in the track record of individual brands, similarly to strong custodial brands in the traditional banking sector.

Hot Storage

Multi-party computation storage is hot storage, meaning the wallet is connected to the internet. This leaves the wallet open to hacks, malware and loss of funds. Some of these online devices are also mobile, which presents a serious risk as the key material is now stored on a device that is inherently insecure.

Hardware Security Module

As of writing, there are no industry-grade HSM's with multi-party computation support. With an HSM, key material is protected creating an additional layer of security. Because multi-party computation does not use HSM's at this time, there is risk of hack or loss of the key material.

Accountability

As noted above, accountability is critical in the transfer of any type of asset. An institution holding cryptocurrencies must be able to track each transaction and have a record of who signed on any given asset transfer.

With multi-party computation, it is impossible to distinguish which of the key parts were used to sign a transaction using only publicly available data from the blockchain. The resulting signature after multi-party computation operations is a signature that appears identical to a single-signature system. There is no on-chain way to discern which of the multi-party computation keys were used or not used to sign a transaction. This can present a problem for institutions in a number of ways:

- **People:** Key materials can be stored by multiple executives at a company. For instance, if six executives hold keys, but only two are required to validate a transaction, it is impossible to know and trace who was responsible for a transaction.
- **Compliance:** Key material could be stored at separate locations. If three private keys are required from storage in five locations, a critical part of compliance would be knowing which of the locations had participated in the transaction.
- **Multi-institutional security:** Key material may be stored at separate institutions. Similar to the first two examples, it would be critical to know who is holding a backup key and which keys are used in a transaction.

Without on-chain accountability, even good actors are put in a difficult position in the case of theft because they have no deniability that their keys were not used.

Leveraging Multi-Party Computation

BitGo has a long track record of helping clients transact securely at scale. BitGo believes there are some current useful applications of multi-party computation technology.

- **Option for Single-Signature Blockchains:** A limited number of blockchains, such as Binance coin, do not provide the primitive capabilities that allow for the validation of multiple keys behind a transaction. In such cases, multi-party computation can be used as a fallback option to mitigate the single point of failure, since there is no more mature solution available.
- **Additional Security Layer:** Multi-Signature wallets with cold storage are an industry standard combination today. Instead of replacing this battle-tested solution, providers are testing adding multi-party computation as an additional layer to multi-signature protocol.



05 Conclusion

At BitGo, our clients are fiduciaries that require the highest level of security. BitGo's layered security approach includes technology, people, processes, and physical security to provide our clients with institutional-grade custody. As an institution on the cutting edge of digital asset security, BitGo has long believed that security is never done, and we are always actively researching new security protocols. We are currently investigating multi-party computation, and would consider applying multi-party computation when it is proven to be an additive security feature.