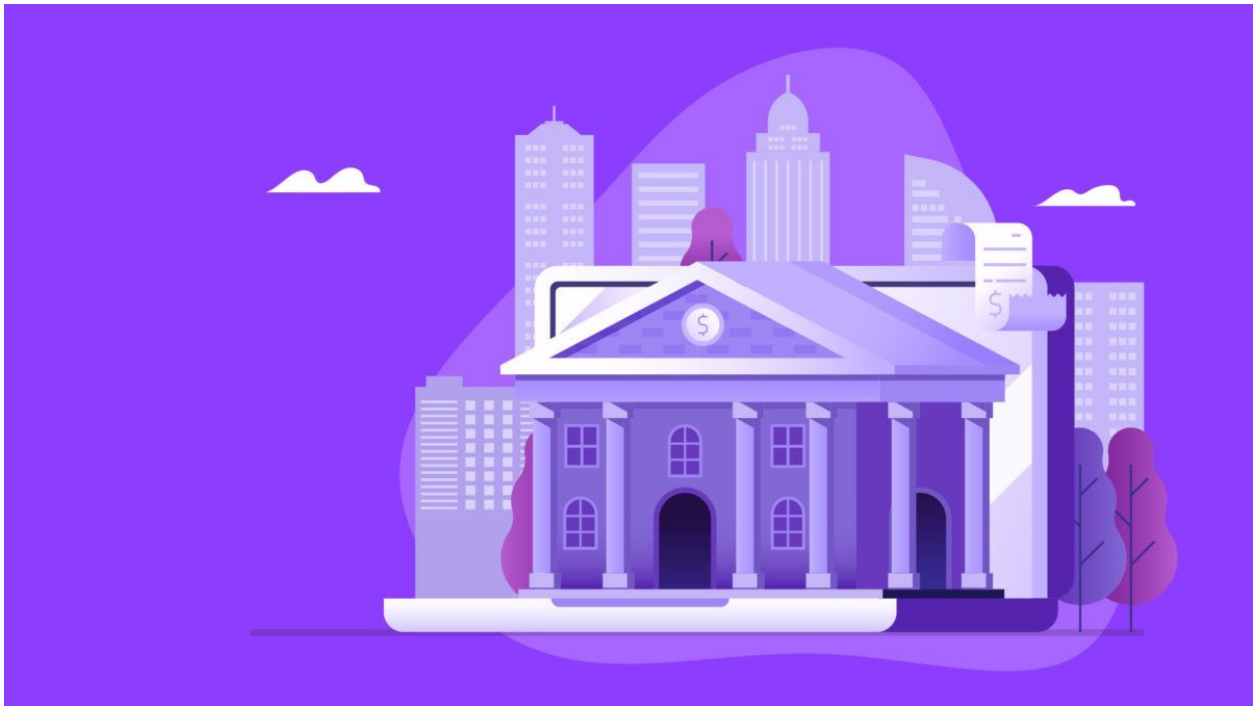
October 1, 2019

Firms reconsider custodian partnerships as tech debate over how to secure digital assets escalates

By Celia Wan



Quick Take

- Recently, debates over whether multi-party computation (MPC) or multi-signature is more secure in storing private keys intensified
- Several companies have “moved away” from multi-signature adopters like BitGo and Unchained Capital to newer firms that deploy MPC, sources told The Block

- Although some firms think that a combination of MPC and multi-signature is the most secure way to store private keys, others believe that these two cryptographic techniques are a zero-sum game

At first glance it seems like an innocent tech debate over how to securely store cryptocurrencies; the main point of contention being: “is multi-signature or multiple-party computation (MPC) better at securing digital assets?”

This nerdiest of turf wars then results in several OTC desks and crypto-native firms shifting away from custodial services using multi-signature, like those offered by BitGo, and forming partnerships with newer firms that adopt MPC, several sources close to the matter told The Block.

“We are seeing a number of clients [that used to adopt multi-signature solutions] move to us,” said a source working for a digital asset security firm. “There are other custodians that are picking up that business as well.”

Shifting away

In an early September blog post[1], BitGo CEO Mike Belshe pointed out several flaws of MPC, concluding that MPC could be used in addition to multi-signature, but not as a stand-alone security solution. “The strongest security for digital wallets today remains with multi-signature wallets,” as he concludes at the end of the blog post.

The post was published during a time when a few newly emerged companies that deploy MPC have already gained traction in the cryptocurrency market. Genesis Trading, which has been using BitGo as its custodian, recently partnered with MPC deployers Curv and Fireblocks, according to several sources close to the matter and the two companies’ websites. Galaxy Digital

[1] https://blog.bitgo.com/multi-sig-vs-mpc-which-is-more-secure-699ecefc8430

is also “moving away” from BitGo to other MPC solutions, another source told The Block, although the cryptocurrency merchant bank still retains some of BitGo’s services as well.

Additionally, Prime Trust, a cryptocurrency financial institution and a qualified custodian, also opted for MPC when it revamped its custodial solutions. The firm’s CEO Scott Purcell told The Block that as a competitor of BitGo, Prime Trust has conducted “extensive diligence on Curv, Ledger Vault, Fireblocks, and others,” before choosing Fireblocks as their technology provider to deploy MPC on its own custodial system.

To be sure, multi-signature and MPC can be used together, especially when companies want to use both cold and hot storage. Cryptocurrency agency brokerage Tagomi, which uses BitGo as one of its cold storage custodians, is also exploring MPC in order to secure its hot wallets.

Meanwhile, GSR Trading has also expressed support for both MPC and multi-signature, as it “sees benefits of both methods,” said GSR trading co-founder Rich Rosenblum to The Block.

“In regards to custodying funds, history has usually sided with Goliath. Yet, it’s still early innings. No company has hit the $10 billion marker yet for digital asset custody,” Rosenblum added, referring to BitGo’s early entrance into the cryptocurrency custody market.

Zero-sum game?

Although firms shopping for custodians may benefit from both cryptographic techniques, some believe that MPC and multi-signature are a zero-sum game.

In multi-signature, a transaction is only authorized after it is signed by several private keys connecting to the same wallet addresses. These keys can be stored in vaults, or the so-called cold storage, to preempt cyberattacks. Meanwhile, MPC generates random key shares instead of a fixed private key. These key shares are stored and computed separately to collectively derive an output that can authorize a transaction.

According to Belshe, one of the major flaws of existing MPC solutions is that currently MPC key shares cannot be stored securely on a physical device, or the so-called Hardware Security Modules (HSMs). Multi-signature custody is safe in the sense that some private keys can be stored on physical devices and only send out signals when signing a transaction without revealing the actual keys. This makes cyberattacks almost impossible. In comparison, although it is feasible to store MPC key shares on physical devices, signing a transaction needs direct access to these key shares, exposing information of the devices and rendering it vulnerable to hacks.

“The main claim against MPC today is the fact that all the parts [key shares] need to be online to do the signature, whereas in cold you can have parties that are offline so you can limit the cybersecurity threat coming in,” a market insider told The Block under the condition of anonymity.

As a result, some firms choose to use multi-signature cold storage in addition to securing their hot wallets with MPC. However, the market insider also pointed out that even though storing keys offline can prevent potential cyberattacks, human errors still existing in storing and retrieving private keys.

Meanwhile, multi-signature also faces its own drawbacks. Multi-signature is only supported by a selective group of blockchains, making it difficult for some businesses to scale their cryptocurrency offerings. Even ethereum, one

of the most popular blockchains, does not support multi-signature natively. Current multi-signature solutions on ethereum are based on smart contracts, which might be vulnerable to cyberattacks. In comparison, MPC is blockchain agnostic, allowing firms to secure tokens built on any chains.

“Not all cryptocurrency protocols support Multi-Sig and those who do, have very different implementations from one another. This makes it more difficult for Multi-Sig providers to support new chains,” said Fireblocks CTO and cofounder Idan Ofrat.

“We do not currently support coins that don’t support multi-sig because we are limited by what those blockchains support,” said BitGo security engineer Lance Vick. “However, we are in the process of developing a solution to bring the security of multi-sig to blockchains that only support single-sig.”

For some, this is an already sufficient reason to adopt MPC, despite all the dispute over which technique is more secure.

“Don’t get me wrong, multi-sig is extremely secure,” said Prime Trust chief product officer Kevin Lehtiniitty. “It’s our position that MPC is as secure and supports way more tokens so it’s the approach we’ve gone with.”

As for BitGo, the long-standing cryptocurrency custodian might finally be exploring MPC as well, despite remaining concerns with this technology.

“Our concern with MPC is that while the technology has been around for a while, current implementations for cryptocurrencies have not had sufficient review or testing to be ready to secure actual funds,” said Vick.

However, “BitGo is always exploring technologies and we are looking at MPC,” BitGo vice president of marketing Clarissa Horowitz told The Block.

Despite the apparent shifting technological winds, Horowitz said the firm has not seen any sort of client exodus.

“BitGo has not lost a single client to custody firms employing MPC. Our concern is that MPC is being inaccurately marketed and deployed without sufficient public code auditing and real-world testing,” she said.

“As it exists today, MPC is too immature to be a viable replacement for multi-sig. We will be continuing to evaluate MPC for future use cases as the technology matures. Establishing trust in new cryptography takes a lot of time and public review, and, therefore, should be approached with patience and caution – especially when it is being used to secure assets of value.”