MPC (Multi-Party Computation)

Multi-signature wallets have become the standard for institutions managing cryptocurrencies as they enhance the security of assets over single key wallets. Recently, however, new cryptographic breakthroughs in MPC are ushering in a new generation of key management. But as the case with most technological developments, misinformation and confusion are common in the early days. MPC and threshold signatures have surpassed multi-sig technology and ultimately deliver on the flexibility and security required to become the next generation of private key security.

Similar to a Multi-Signature configuration, a private key within an MPC-based solution is never created or held in one single place. MPC technology protects the key from being compromised by both cybercriminals and from internal fraud and collusion, preventing any employee, or group of employees, from stealing the digital assets.

MPC works on the standardized cryptographic signature algorithm (ex. ECDSA) that is used across most blockchains, making the implementation of MPC possible between different blockchains. This means that institutions that utilize MPC can quickly and easily onboard new cryptocurrencies onto their platform.

While MPC technology was only applied within the cryptocurrency wallet context relatively recently, it has been the topic of academic research since the early 1980s and has undergone extensive, public peer reviews. As the MPC implementation is agnostic to the blockchain protocol, the attack surface is minimal and each review fixes implementation for all the protocols. Unfortunately, this is not the case with an on-chain Multi-Sig solution, as each protocol requires the wallet provider to implement a different code.

MPC allows for ongoing modification and maintenance of the signature scheme. For example, changing from a '3 of 4' set-up to any other set-up would 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: 1. you don't need to create a new wallet; 2. you don't need to move any funds; 3. your counterparties can continue to use the existing address

MPC-based wallets are represented on the blockchain as a single wallet address, with the actual distributed signature computed outside of the blockchain. This translates into having the lowest fees possible for the transaction.

Accountability is probably one of the most misunderstood aspects of an MPC-based solution. MPC provides off-chain accountability so that each co-signing component can audit which of the keys participated in the signing without it being made public to outsiders. Solutions based on MPC are able to provide a thorough and trustworthy record to allow for true accountability.

Hardware Isolation Modules (HSMs and Secure Enclaves) are an important means of protecting cryptographic material when the system is compromised. But HSMs alone are not sufficient for providing the most secure solution to protecting your private key. Likewise, MPC alone is only part of the solution. As a result, this has given rise to a misconception that both MPC and HSMs are substitutional technologies. Instead, the use of MPC in addition to hardware isolation systems, such as HSMs, is critical because HSMs alone are not completely bullet-proof.

Institutions know that in order to be competitive, there can be no compromises between security and accessibility. MPC technology allows for businesses to capture market opportunities and deploy their digital assets in a secure environment that simply was not possible before.