What is MPC (Multi-Party Computation)?

If you’re in the institutional digital asset space, you’ve probably heard about MPC (multi-party computation). While MPC theory has been around since the early ’80s, it first entered the digital asset space just a few years ago; since then, MPC has become one of the primary technologies wallet providers and custodians are utilizing to secure crypto assets.

But what exactly *is*MPC? How does it work, and what benefits does it have?

## **Introduction to Cryptography**

## The field of cryptography provides its users with a method for:

* sending messages that only the intended receiver of the message will understand
* preventing unauthorized third parties from reading them in case of interception
* verifying the authenticity and integrity of digital messages from a known sender
* Cryptography was once primarily the concern of government and military agencies, in the internet era cryptography plays an increasingly central role in the way we all transfer information.
* While the idea behind cryptography can appear simple, the field does include some extremely complex math. In essence, messages are scrambled, or “encrypted,” by a secret recipe (or algorithm) that hides the information contained within it. This way, should the encrypted message be stolen or intercepted by a malicious or non-trusted third party, they will be unable to understand, see or alter the information the message holds. Instead, the only one who can read that message correctly is the one who knows how the message was encrypted and thus holds the key to unscramble, or “decrypt,” it.

In the world of blockchain,

MPC solutions must adhere to two main principles:

* Input privacy – the private data held by parties collaborating to build a combined output cannot be inferred or deduced
* Correctness – the output obtained is always correct and parties should not be able to influence an incorrect output

The “message” being transferred is a digital asset, and the “key” to that digital asset is essentially the decryption tool used to receive that digital asset.

* That key itself – known as the “private key,” as access to a digital asset requires both a publicly known cryptographic key and a related private one – must be kept safe, as anyone who knows the private key can move the asset to their own wallet. This is where MPC comes in: it’s one of the most powerful tools for protecting private keys.

## **How does MPC (multi-party computation) work?**

MPC enables multiple parties – each holding their own private data – to evaluate a computation without ever revealing any of the private data held by each party (or any otherwise related secret information).

The two basic properties that a multi-party computation protocol must ensure are:

* **Privacy:** The private information held by the parties cannot be inferred from the execution of the protocol.
* **Accuracy:** If a number of parties within the group decide to share information or deviate from the instructions during the protocol execution, the MPC will not allow them to force the honest parties to output an incorrect result or leak an honest party’s secret information.

In an MPC, a given number of participants each possess a piece of private data (d1, d2,dN). Together, the participants can compute the value of a public function on that private data: F(d1, d2, dN) while keeping their own piece of data secret.

 MPC is utilized for a number of practical applications, such as electronic voting, digital auctions, and privacy-centric data mining. **One of the top applications for MPC is for securing digital assets – and recently, MPC has become the standard for institutions looking to secure their assets while retaining fast and easy access to them**.

Zero Knowledge Proof (ZKP), a technique by which a prover can convince the verifier of a fact without revealing the actual content, are leveraged. ZKP operates on three basic tenets:

* Completeness – If a statement is true then the verifier will be convinced that prover possesses the correct input
* Soundness – If a statement is false then no dishonest prover can convince verifier that they have the correct input
* Zero knowledge - if a statement is true then no verifier learns anything other than the fact that the statement is true

### **MPC for Private Key Security**

With MPC, private keys (as well as other sensitive information, such as authentication credentials) no longer need to be stored in one single place. The risk involved with storing private keys in one single location is referred to as a “single point of compromise.” With MPC, the private key is broken up into shares, encrypted, and divided among multiple parties.

These parties will independently compute their part of the private key share they hold to produce a signature without revealing the encryption to the other parties. This means there is never a time when the private key is formed in one place; instead, it exists in a fully “liquid” form.

Ordinarily, when a single private key is stored in one place, a wallet’s owner would need to trust that the device or party that holds that private key is completely secure. Such a crypto exchange that essentially holds the customer’s private keys on their behalf.

However, these parties have proven themselves to be vulnerable. When an attacker only needs to succeed in hacking one point of compromise to steal a private key, it leaves the digital assets that key unlocks wide open to theft.

MPC does away with this problem, as the private key is now no longer held by any one party at any point in time. Instead, it is decentralized and held across multiple parties (i.e. devices), each blind to the other. Whenever the key is required, MPC is set in motion to confirm that all parties, or a predetermined number of parties out of the full set, approve of the request.  
  
With MPC technology in play, a potential hacker now has a much harder task ahead of them. To gain control over a user’s wallet, they now need to attack multiple parties across different operating platforms at different locations simultaneously.

Source - <https://www.wipro.com/blogs/hitarshi-buch/establishing-blockchain-privacy-through-zero-knowledge-proof/>

<https://www.wipro.com/blockchain/synergizing-blockchain-and-multi-party-computation-to-reimagine-transactions/>

<https://www.fireblocks.com/what-is-mpc/>