multisig, MPC, secret sharing, ...

in-house seminar

Jeongho Jeon

2025-03-XX

DSRV (All That Node, Custody, Payments, Validator, WELLDONE Studio)

version 20250411

Intro

We sign transactions to prove cryptocurrency ownership or the authority to manage it. In many cases, a single private key is used for signing, but there is a risk of key loss or leakage. To mitigate this, the key is split into multiple parts, and combine them to generate a signature.

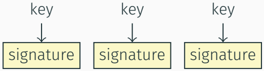
multisig, MPC wallet, secret sharing, threshold signature

The terms are frequently misused interchangeably, but there are differences.

multisig (multi-signature)

Typically multisig creates separate signatures using unrelated keys and concatenates them without any special cryptographic techniques.

Bitcoin has built-in multisig support, `OP_CHECKMULTISIG`. Blockchains with smart contracts can implement multisig smart contracts (e.g., Ethereum's Gnosis Safe). Cosmos SDK supports nested multisigs.

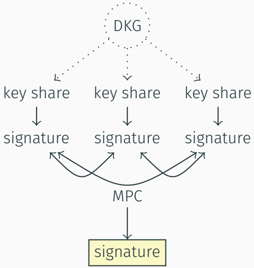


Compared to other methods, it allows for easier weighting. (e.g., requiring a total of 3 or more votes when A has 3, B has 2, and both C and D have 1 vote).

MPC (multi-party computation)

MPC is a cryptographic field where participants encrypt their secrets, exchange them, and compute results. For example, encrypted salaries can be aggregated to calculate the average salary. Beyond signatures, it is used in voting, auctions, medical data analysis, demographic surveys, and more.

Each participant signs with their own key, and these signatures are combined to compute the final signature. It is indistinguishable whether it was created using a single private key or multiple keys. Since wallets aggregate multiple signatures, there is only a single signature on-chain.



MPC (multi-party computation)

This enables geographically separated individuals to sign securely online. However, participants are often required to be online simultaneously.

DKG (Distributed Key Generation) eliminates the need to trust a key generator.

Different signature methods (ECDSA, EdDSA, …) require different MPC algorithms.

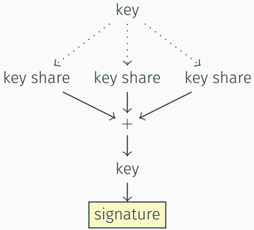
secret sharing

It is often referring to the most common Shamir secret sharing method. A certain number of private key shares are combined to reconstruct the private key, which is then used to sign.

Similar to MPC, it is indistinguishable whether the signature is made with one private key or several keys just by a signature.

Since the private keys are combined before signing, it is signature method agnostic.

There is a risk of key exposure during the signing process.



threshold signature

Threshold signature is the method where t of n must come together to create a signature. Most multisig, MPC, and secret sharing are threshold signature schemes (TSS).

related terms

key rotation allows for the generation of new key if some keys are lost or compromised. Even if there is no issue with keys, we change keys periodically for security reasons.

reconfiguration regenerates keys when the signing participants change.

signature aggregation Multiple signatures are aggregated to create a single signature. This saves blockchain storage and reduces the verification time during blockchain consensus process.

HSM (Hardware Security Module) Commonly known as a hardware wallet. It signs transactions with stored private key without revealing the key itself.

related terms

DVT (Distributed Validator Technology) Validators sign blocks they propose and blocks created by others to acknowledge the validity of blocks. If validators fails to sign on time due to hardware or software issues, they may face penalties (inactive slashing). To protect against failures, redundant servers may be used, but this introduces the risk of double slashing, where two different signature are published.

To address this, multiple servers sign each, and the signatures are aggregated to produce a final signature, which is to be published. Examples include Obol and SSV on Ethereum. They use BLS signature aggregation within their own signature-making network.