Multisig

Sui supports multi-signature (multisig) transactions, which require multiple keys for authorization rather than a single, one-key signature. In technical terms, Sui supports k out of n multisig transactions, where k is the threshold and n is the total weights of all participating parties. The maximum number of parties is 10. To learn more about the single key signatures that Sui supports, see Signatures .

Valid participating keys for multisig are Pure Ed25519, ECDSA Secp256k1, and ECDSA Secp256r1. A (u8) weight is set for each participating keys and the threshold can be set as u16 . If the serialized multisig contains enough valid signatures of which the sum of weights passes the threshold, Sui considers the multisig valid and the transaction executes.

Sui allows you to mix and match key schemes in a single multisig account. For example, you can pick a single Ed25519 mnemonic-based key and two ECDSA secp256r1 keys to create a multisig account that always requires the Ed25519 key, but also one of the ECDSA secp256r1 keys to sign. You could use this structure for mobile secure enclave stored keys as two-factor authentication.

Currently, iPhone and high-end Android devices support only ECDSA secp256r1 enclave-stored keys.

Compared to threshold signatures, a multisig account is generally more flexible and straightforward to implement and use, without requiring complex multi-party computation (MPC) account setup ceremonies and related software, and any dependency in threshold crypto providers. Additionally, apart from the ability to mix and match key schemes and setting different weights for each key (which is complex in threshold cryptography), multisig accounts are "accountable" and "transparent" by design because both participating parties and observers can see who signed each transaction. On the other hand, threshold signatures provide the benefits of hiding the threshold policy, but also resulting in a single signature payload, making it indistinguishable from a single-key account.

Multisig structures supported in Sui.

Applications of multisig

Sui allows you to mix and match key schemes in a single multisig account. For example, you can pick a single Ed25519 mnemonic-based key and two ECDSA secp256r1 keys to create a multisig account that always requires the Ed25519 key, but also one of the ECDSA secp256r1 keys to sign. You could use this structure for mobile secure enclave stored keys as two-factor authentication.

Currently, iPhone and high-end Android devices support only ECDSA secp256r1 enclave-stored keys.

Compared to threshold signatures, a multisig account is generally more flexible and straightforward to implement and use, without requiring complex multi-party computation (MPC) account setup ceremonies and related software, and any dependency in threshold crypto providers. Additionally, apart from the ability to mix and match key schemes and setting different weights for each key (which is complex in threshold cryptography), multisig accounts are "accountable" and "transparent" by design because both participating parties and observers can see who signed each transaction. On the other hand, threshold signatures provide the benefits of hiding the threshold policy, but also resulting in a single signature payload, making it indistinguishable from a single-key account.

Multisig structures supported in Sui.

Related links