BitGo

ETHEREUM TSS

By Oli Beyene

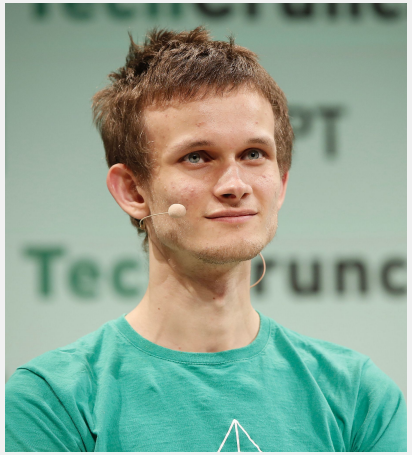
Overview

- Ethereum blockchain
- Ethereum Wallets
- Ethereum Transactions
- Smart Contract Wallets at BitGo
- TSS Wallets at BitGo
- TSS or Smart Contract Wallets
- Developer Portal
- Building Session

Setup

Ethereum Blockchain

- General purpose blockchain
- Proof of Stake



Vitalik Buterin

Ethereum Wallets

- EOA (Externally-owned account)
- Smart Contract

Ethereum Wallets

- Ether
- Address
- Smart Contract
- Transactions

Ethereum Transactions

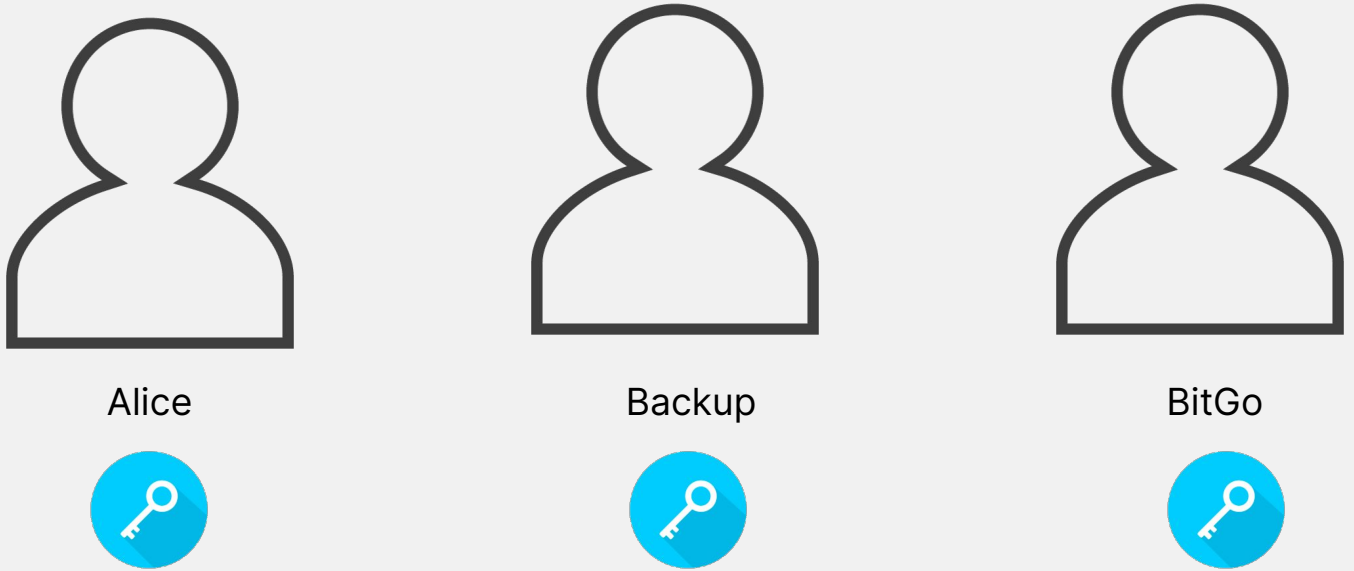
- Recipient
- Value
- Nonce
- Gas Limit
- Max Priority Fee Per Gas
- Max Fee Per Gas
- Data
- Signature

Smart Contract Wallets at BitGo

- Multiple party ownership
- 2 - of - 3

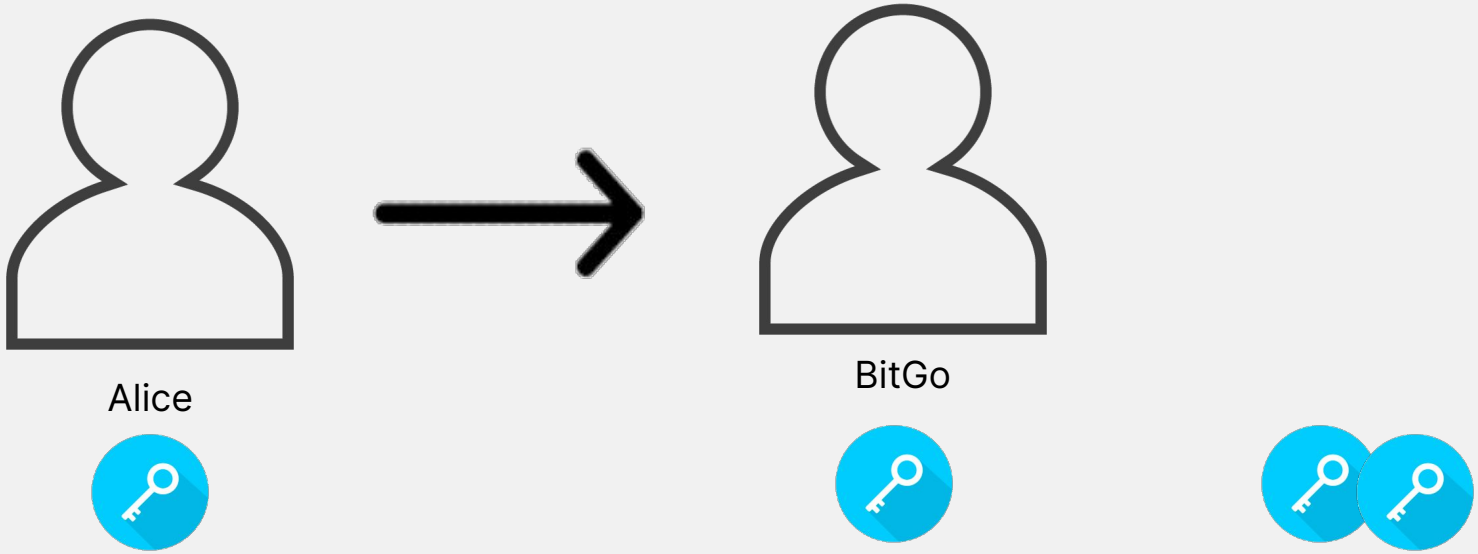
Smart Contract Wallets at BitGo

- Keys



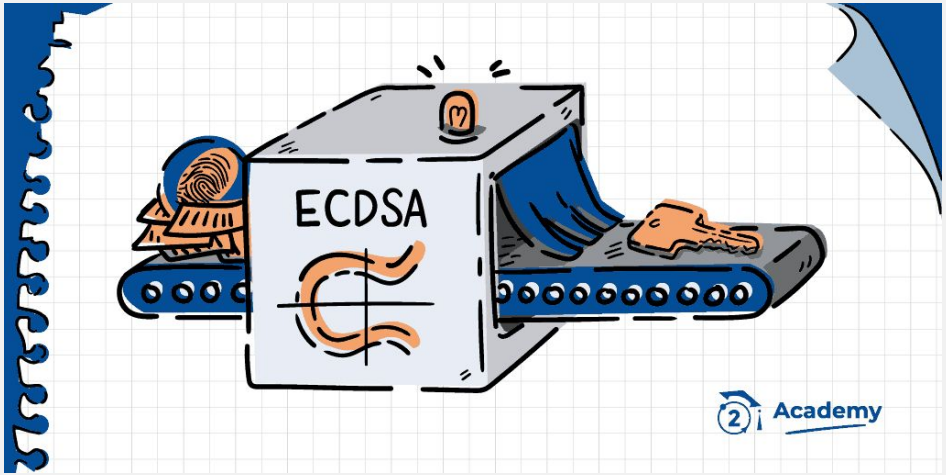
Smart Contract Wallets at BitGo

Smart Contract Wallets at BitGo



TSS Wallets at BitGo

- Threshold Signature Scheme
- Multiparty Computation (MPC)
- 2 - of - 3



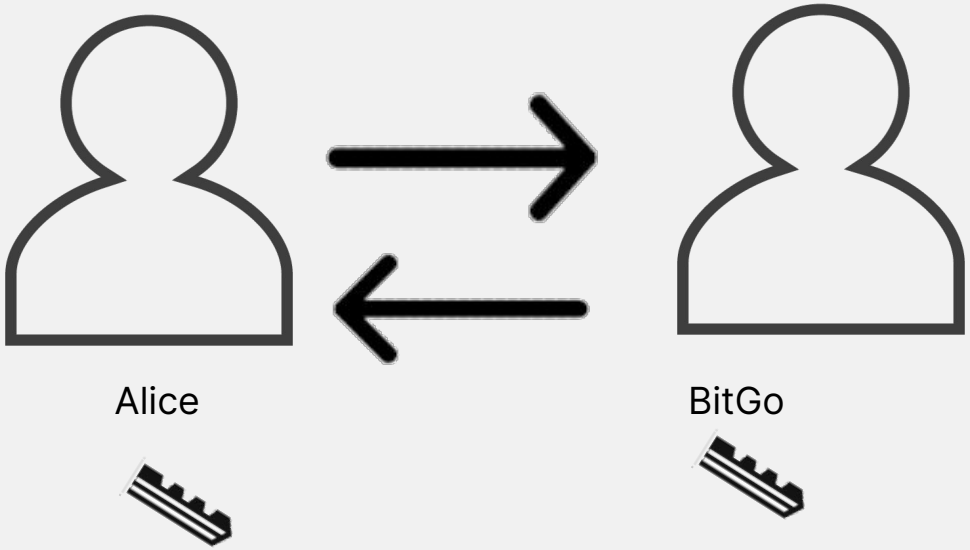
TSS Wallets at BitGo

- Keys

BitGo TSS Wallets

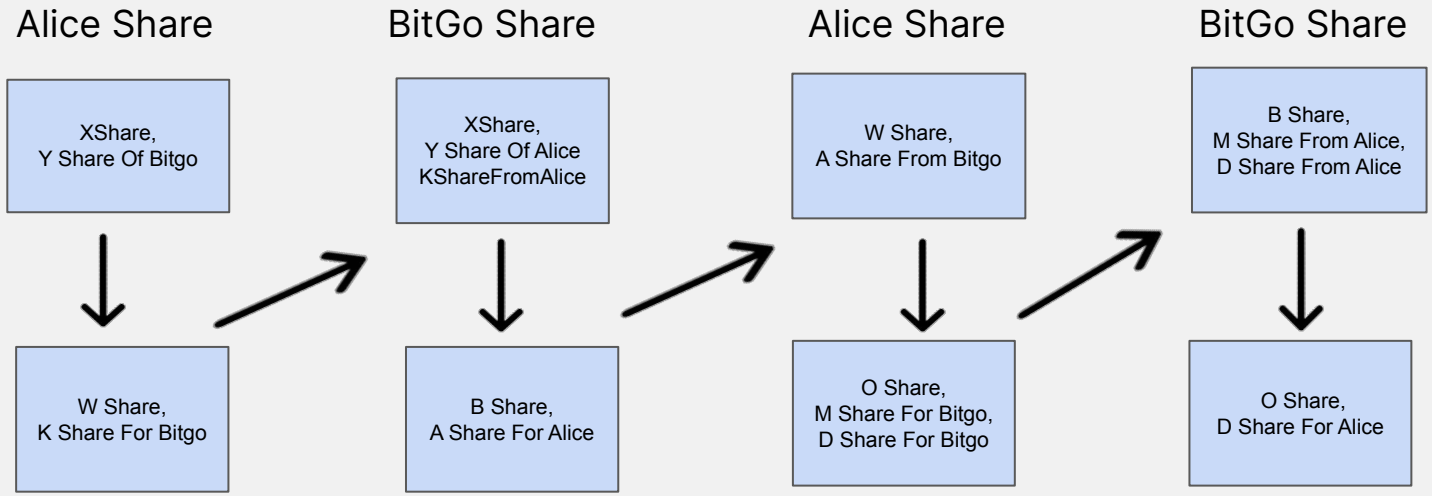
BitGo TSS Wallets

- Signature



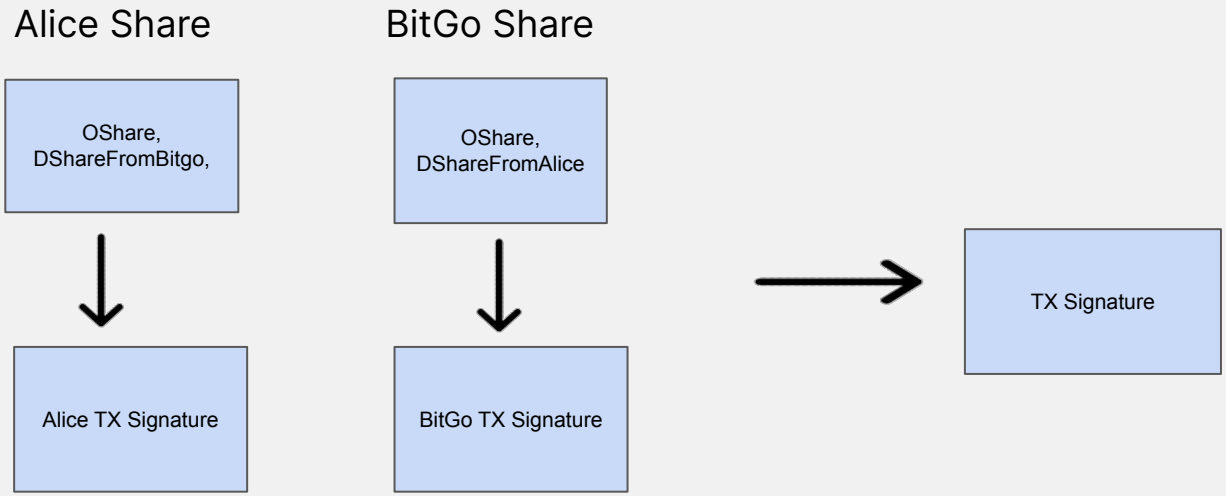
ECDSA MPC

- Signing

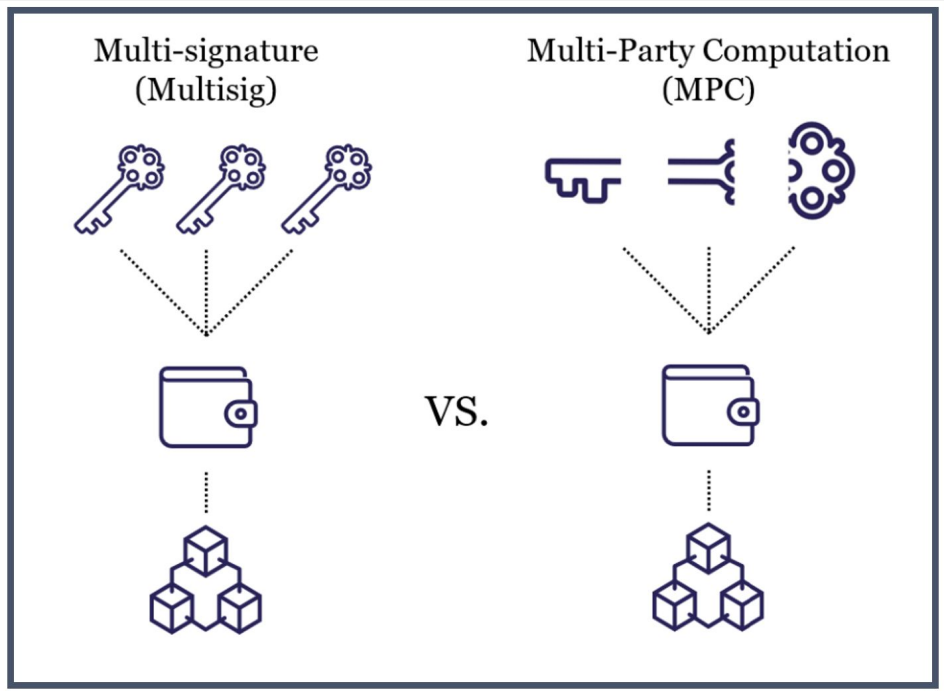


ECDSA MPC

- Signing



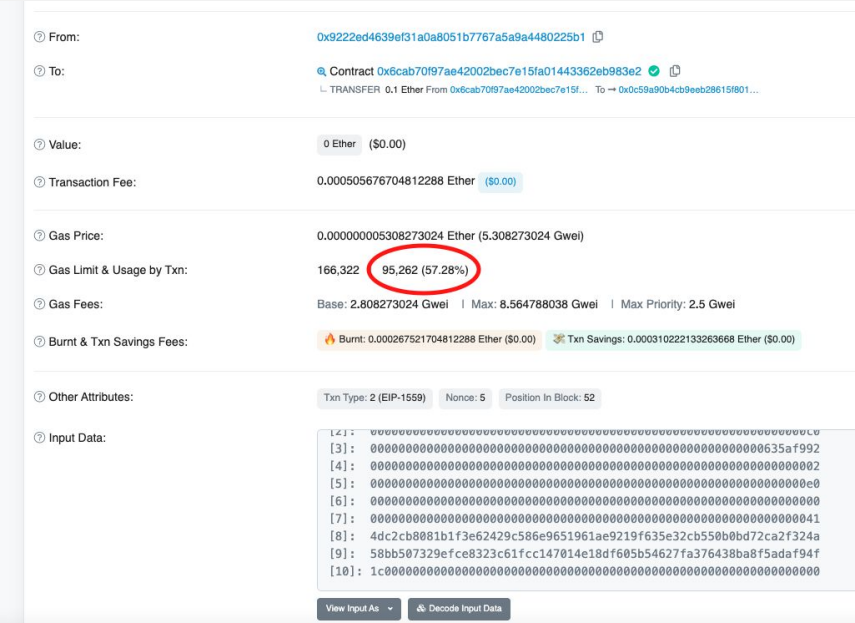
BitGo Smart Contract vs TSS Wallets



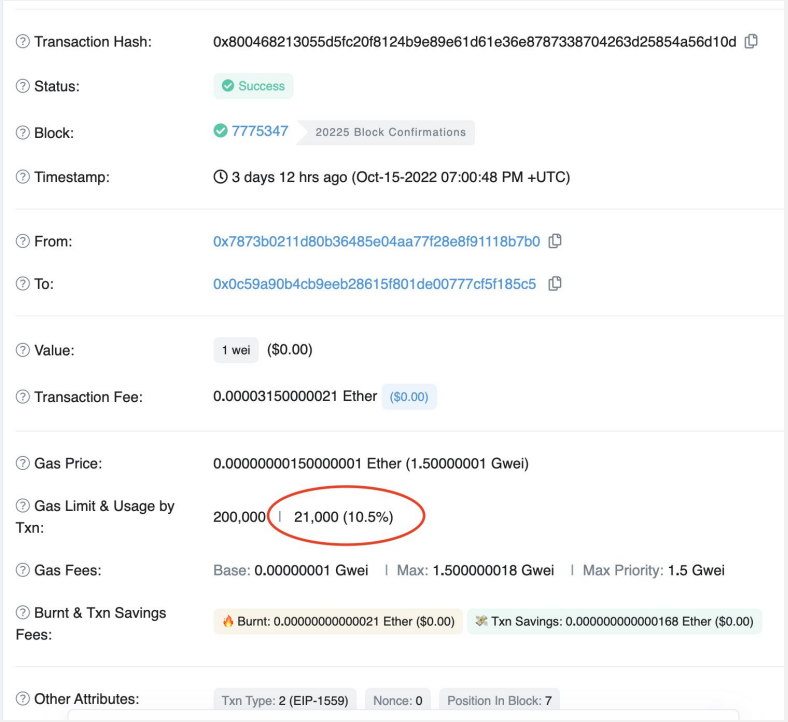
TSS or Smart Contract Wallets

- Secure
- Low Fees

Smart Contract TX



EOA TX



BitGo Developer Portal

- Custody
- Identity
- Liquidity
- Settlement
- Wallet

https://developers.bitgo-dev.com/

Let’s Build