

ETHEREUM TSS

By Oli Beyene

Overview

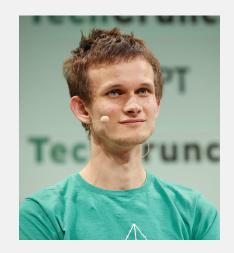
- Ethereum blockchain
- Ethereum Wallets
- Ethereum Transactions
- Smart Contract Wallets at BitGo
- TSS Wallets at BitGo
- TSS or Smart Contract Wallets
- Developer Portal
- Building Session





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

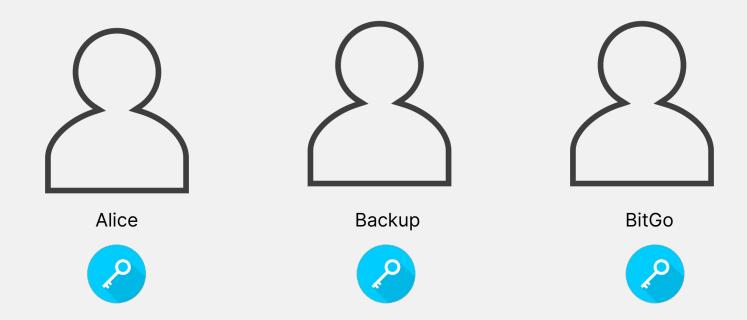
- Recipient
- Value
- Nonce
- Gas Limit
- Max Priority Fee Per Gas
- Max Fee Per Gas
- Data
- Signature

- Multiple party ownership
- 2 of 3

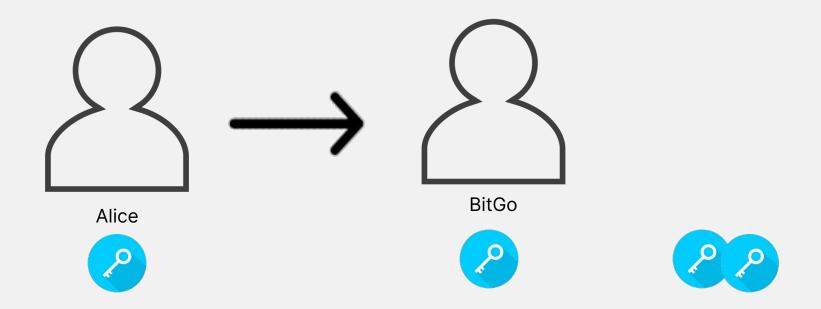




Keys







TSS Wallets at BitGo

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



TSS Wallets at BitGo

Keys

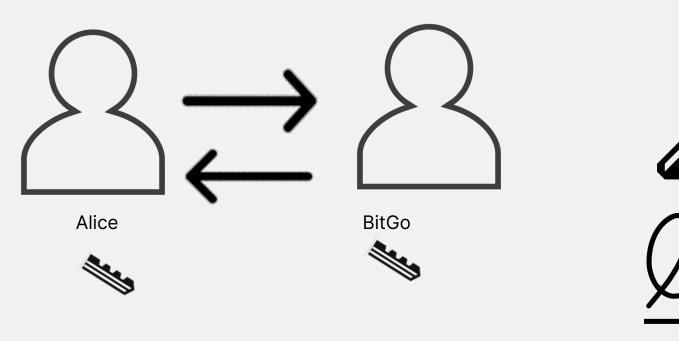


BitGo TSS Wallets



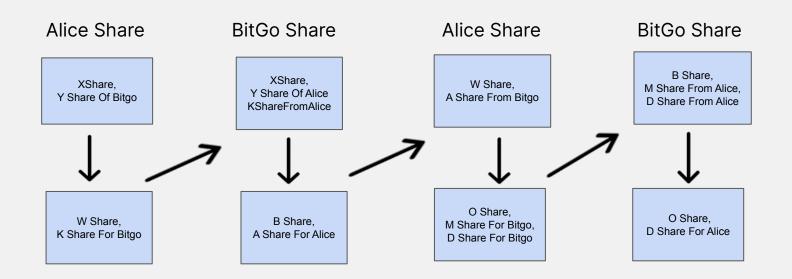
BitGo TSS Wallets

Signature



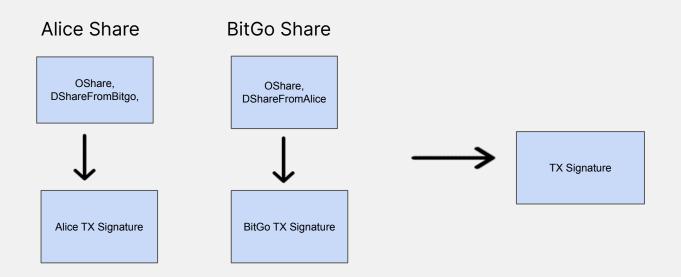
ECDSA MPC

Signing

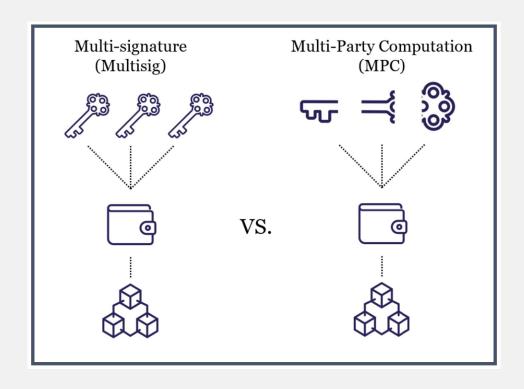


ECDSA MPC

Signing

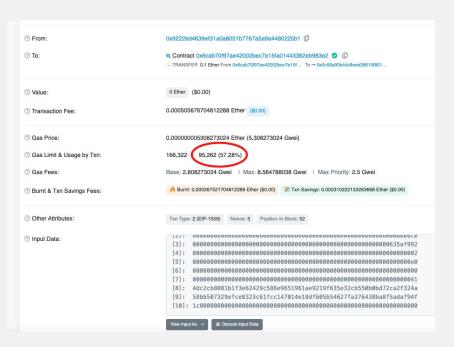


BitGo Smart Contract vs TSS Wallets



TSS or Smart Contract Wallets

- Secure
- Low Fees



EOA TX	⑦ Transaction Hash:	0x800468213055d5fc20f8124b9e89e61d61e36e8787338704263d25854a56d10d 🗓
	③ Status:	⊘ Success
	③ Block:	⊘ 7775347 20225 Block Confirmations
	? Timestamp:	① 3 days 12 hrs ago (Oct-15-2022 07:00:48 PM +UTC)
	⑦ From:	0x7873b0211d80b36485e04aa77f28e8f91118b7b0 (D
	⑦ To:	0x0c59a90b4cb9eeb28615f801de00777cf5f185c5
	⑦ Value:	1 wei (\$0.00)
	⑦ Transaction Fee:	0.00003150000021 Ether (\$0.00)
	⑦ Gas Price:	0.0000000150000001 Ether (1.50000001 Gwei)
	⑦ Gas Limit & Usage by Txn:	200,000 21,000 (10.5%)
	⑦ Gas Fees:	Base: 0.00000001 Gwei Max: 1.500000018 Gwei Max Priority: 1.5 Gwei
	⑦ Burnt & Txn Savings Fees:	♦ Burnt: 0.00000000000021 Ether (\$0.00) ፠ Txn Savings: 0.00000000000168 Ether (\$0.00)
	Other Attributes:	Txn Type: 2 (EIP-1559) Nonce: 0 Position In Block: 7

BitGo Developer Portal

- Custody
- Identity
- Liquidity
- Settlement
- Wallet

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



