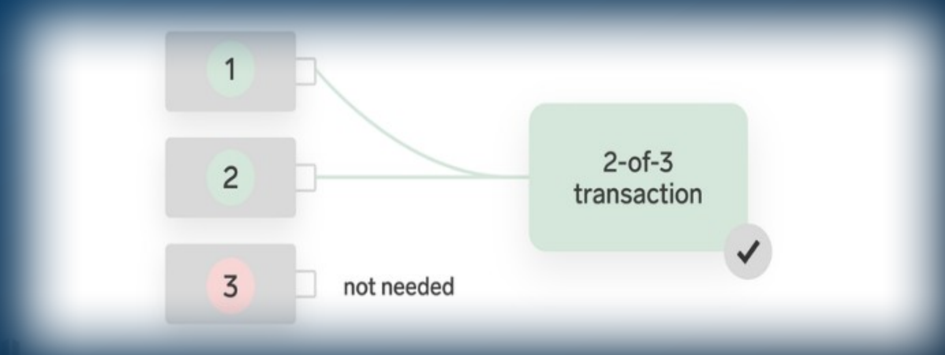
Multi-Signature

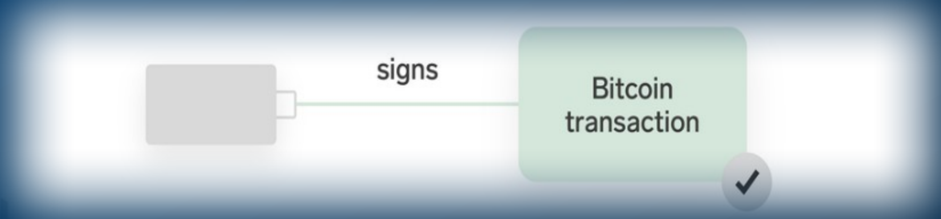
- 🔑What is?
- 🔑Benefits
- 🔑Trade offs
- 🔑Case of use
- 🔑Best Practices
- 🔑Q&A

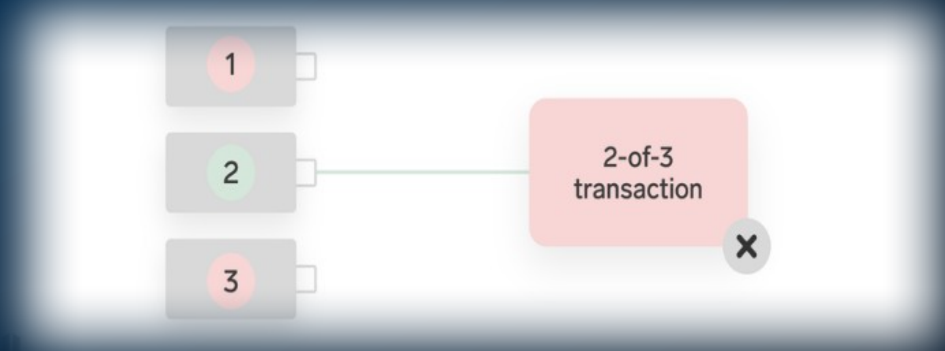
What is

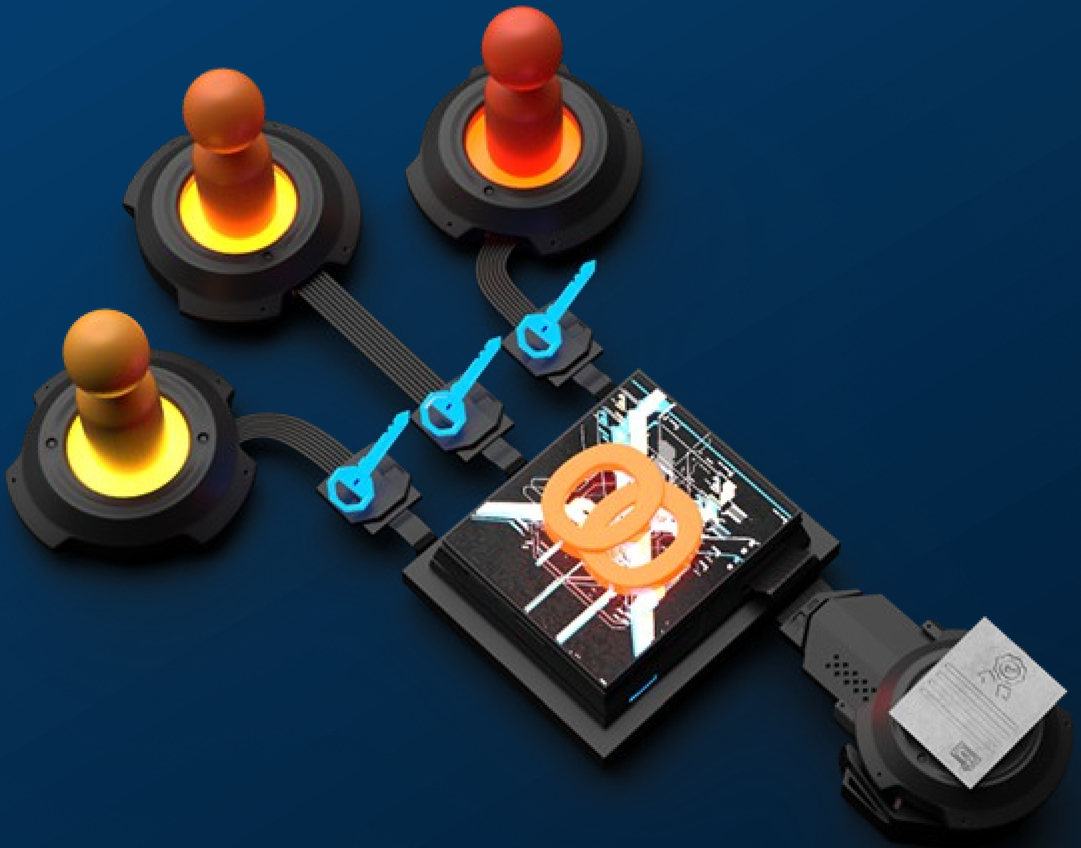
Multi-signature requires several keys to authorize a Bitcoin transaction instead of a single key.

Note: If you use Hodl Hold or Lend, you are utilizing a multisig setup.


1
2
2-of-3
transaction
✓
3
not needed


signs
Bitcoin
transaction
✓


1
2
2-of-3
transaction
✗
3



Benefits

🔑 Enhanced Security

🔑 Shared Control

🔑 Transparency & Accountability

🔑 Safer Long-Term Storage

🔑 Business and Legal Applications

🔑 Customizable Access Models

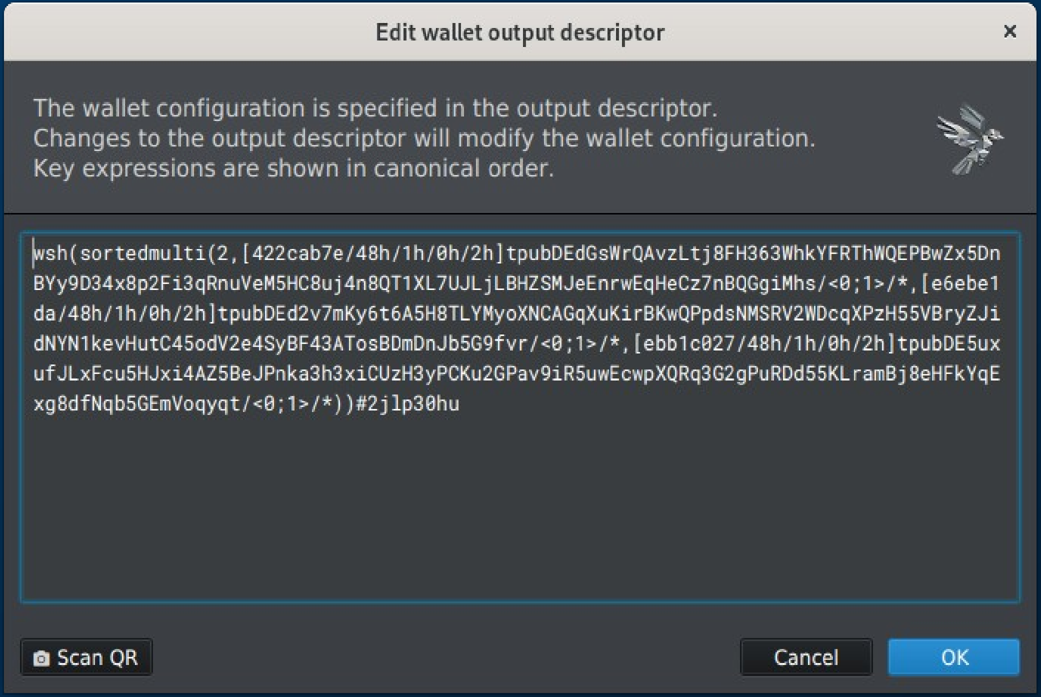
Trade offs

- Complexity: The descriptor is a important piece
- Single Point of Miscommunication
- Reduced Flexibility
- Key Management Risks
- Tooling and Wallet Compatibility
- Higher Transaction Costs

Risks

- Maintain multiple backups
- Store each key’s XPUB
- You cannot switch from single-sig to multisig or viceversa.

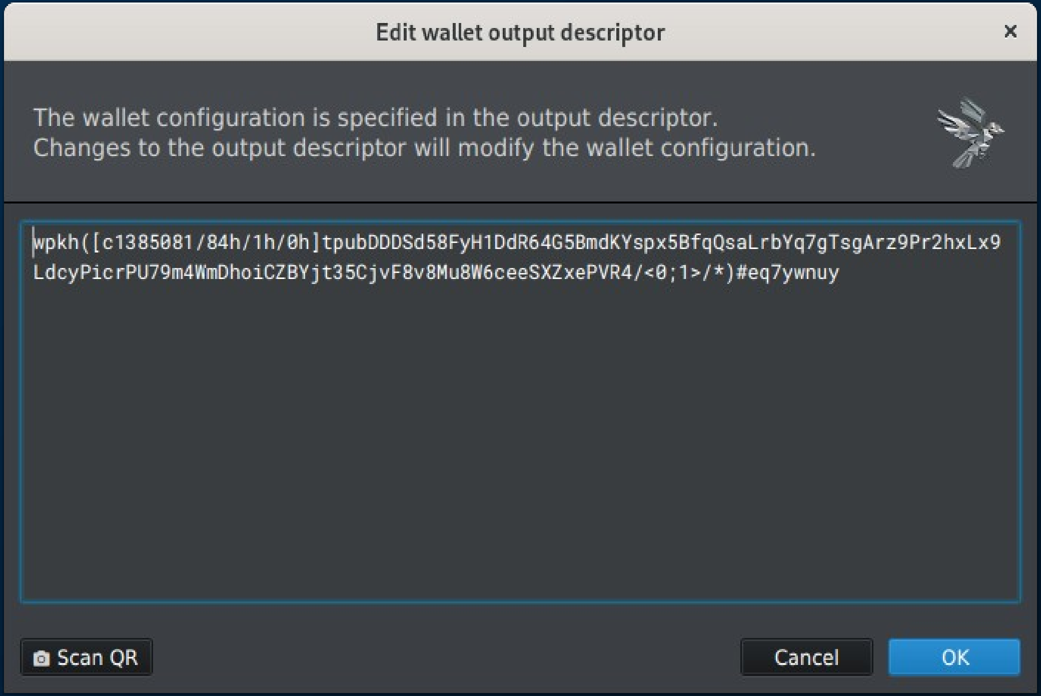
[XTX]



Edit wallet output descriptor

The wallet configuration is specified in the output descriptor.
Changes to the output descriptor will modify the wallet configuration.
Key expressions are shown in canonical order.

```
wsh(sortedmulti(2,[422cab7e/48h/1h/0h/2h]tpubDEdGsWrQAvzLtj8FH363WhkYFRThWQEPBwZx5Dn
BYy9D34x8p2Fi3qRnuVeM5HC8uj4n8QT1XL7UJLjLBHZSMJeEnrwEqHeCz7nBQGgiMhs/<0;1>/*,[e6ebe1
da/48h/1h/0h/2h]tpubDEd2v7mKy6t6A5H8TLYMyoXNCAGqXuKirBKwQPpdsNMSRV2WDcqXPzH55VBryZJi
dNYN1kevHutC45odV2e4SyBF43ATosBDmDnJb5G9fvr/<0;1>/*,[ebb1c027/48h/1h/0h/2h]tpubDE5ux
ufJLxFcu5HJxi4AZ5BeJPnka3h3xiCUzH3yPCKu2GPav9iR5uwEcwpXQRq3G2gPuRDd55KLramBj8eHFkYqE
xg8dfNqb5GEmVoqyqt/<0;1>/*))#2jlp30hu
```



Edit wallet output descriptor

The wallet configuration is specified in the output descriptor.
Changes to the output descriptor will modify the wallet configuration.

```
wpkh([c1385081/84h/1h/0h]tpubDDDSd58FyH1DdR64G5BmdKYspx5BfqQsaLrbYq7gTsgArz9Pr2hxLx9
LdcyPicrPU79m4WmDhoiCZBYjt35CjvF8v8Mu8W6ceeSXZxePVR4/<0;1>/*)#eq7ywnuy
```

Case of use

- Personal Security
- Businesses and Organizations
- Collaborative custody
- Family Wealth Management
- Escrow Services
- Decentralized Autonomous Organizations (DAOs)

Best Practices

- 🔑Test a Mock Setup on Testnet
- 🔑Decide on Spending Rules
- 🔑Configure the Multisig Wallet
- 🔑Generate and Distribute Private Keys Securely
- 🔑Test the Wallet
- 🔑Delete and Re-import the Wallet
- 🔑Repeat Until It's Muscle Memory

Coordinator Software Desktop

- Electrum (They are missing some standards)
- Specter (PGP key is expired since last November)
- Sparrow (It’s the current standard)
- Nunchuck (Desktop version not as good mobile)
- Bitcoin Safe (UX an UI not the best, but FOSS)

Coordinator Software Mobile

- 🔑Blue (IOS and Android)
- 🔑Nunchuck (IOS and Android)
- 🔑Bitcoin Keeper (IOS and Android)

Q&A

RIVACY