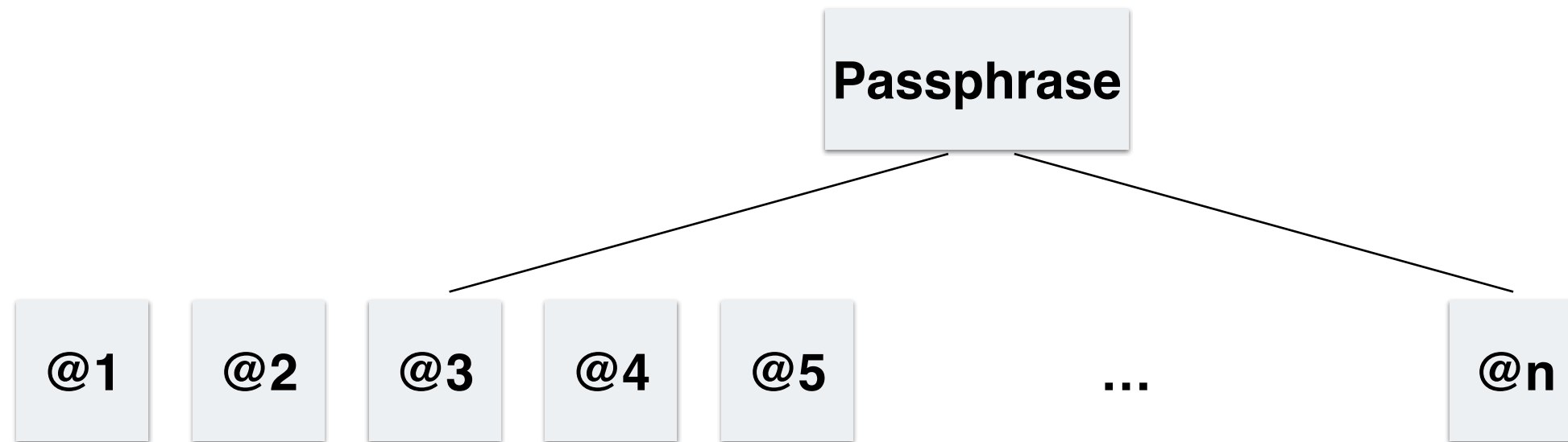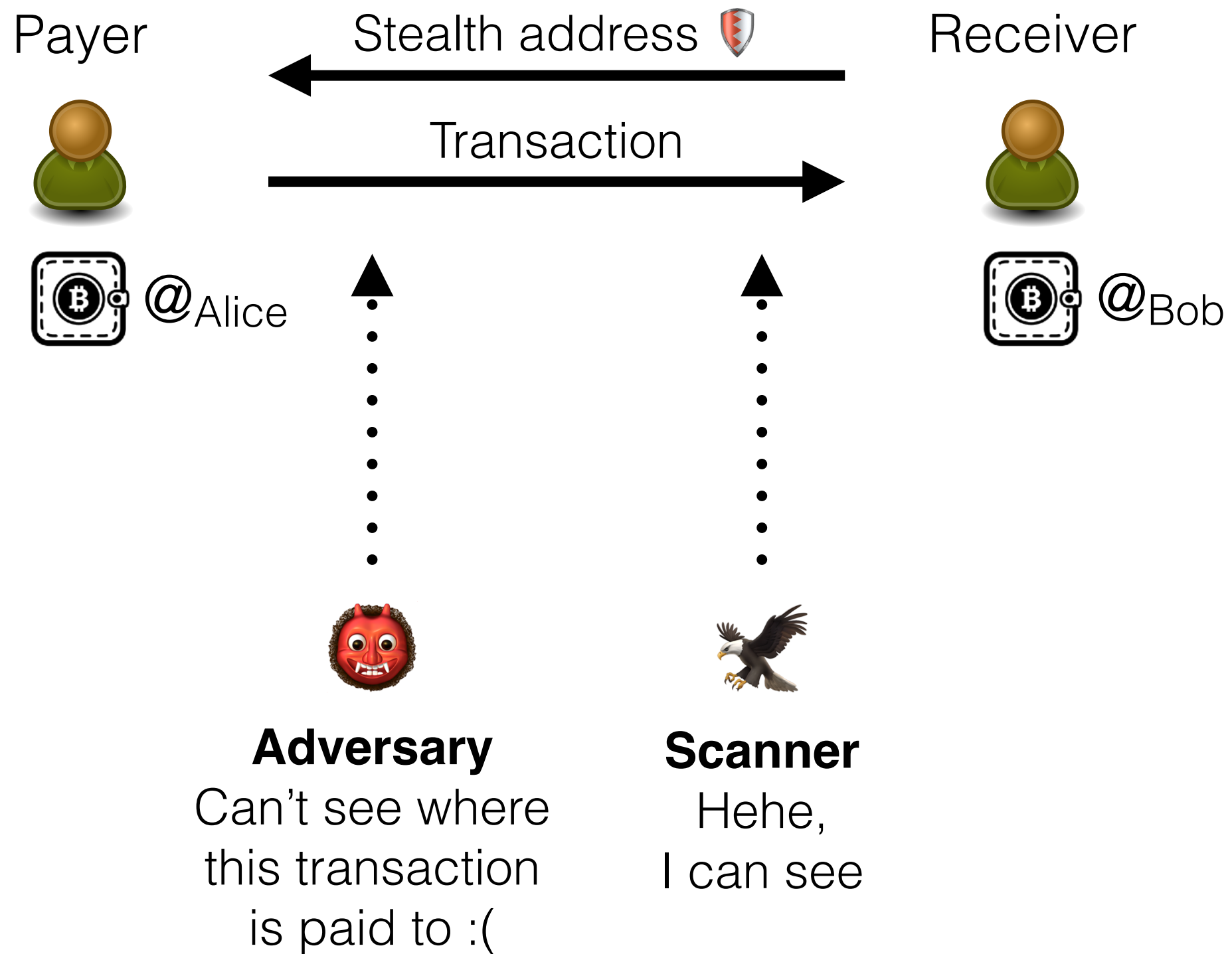**Blockchain Privacy
Stealth Addresses**
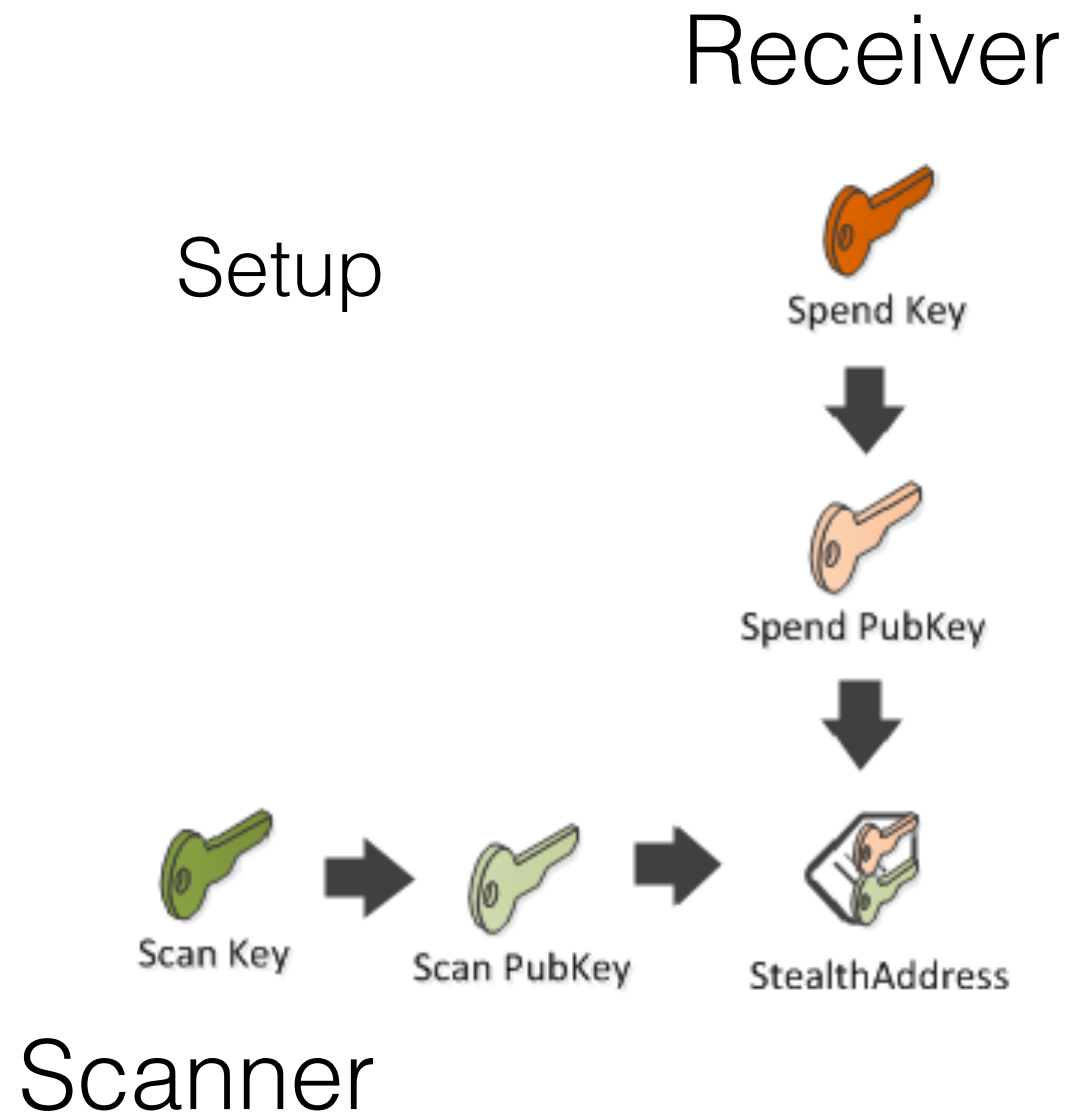
Hierarchical Deterministic (HD) Wallets

- Addresses derived from the same key

- From one address cannot derive the other addresses

- Used by the majority of Bitcoin/Ethereum wallets today

- A form of stealth addresses
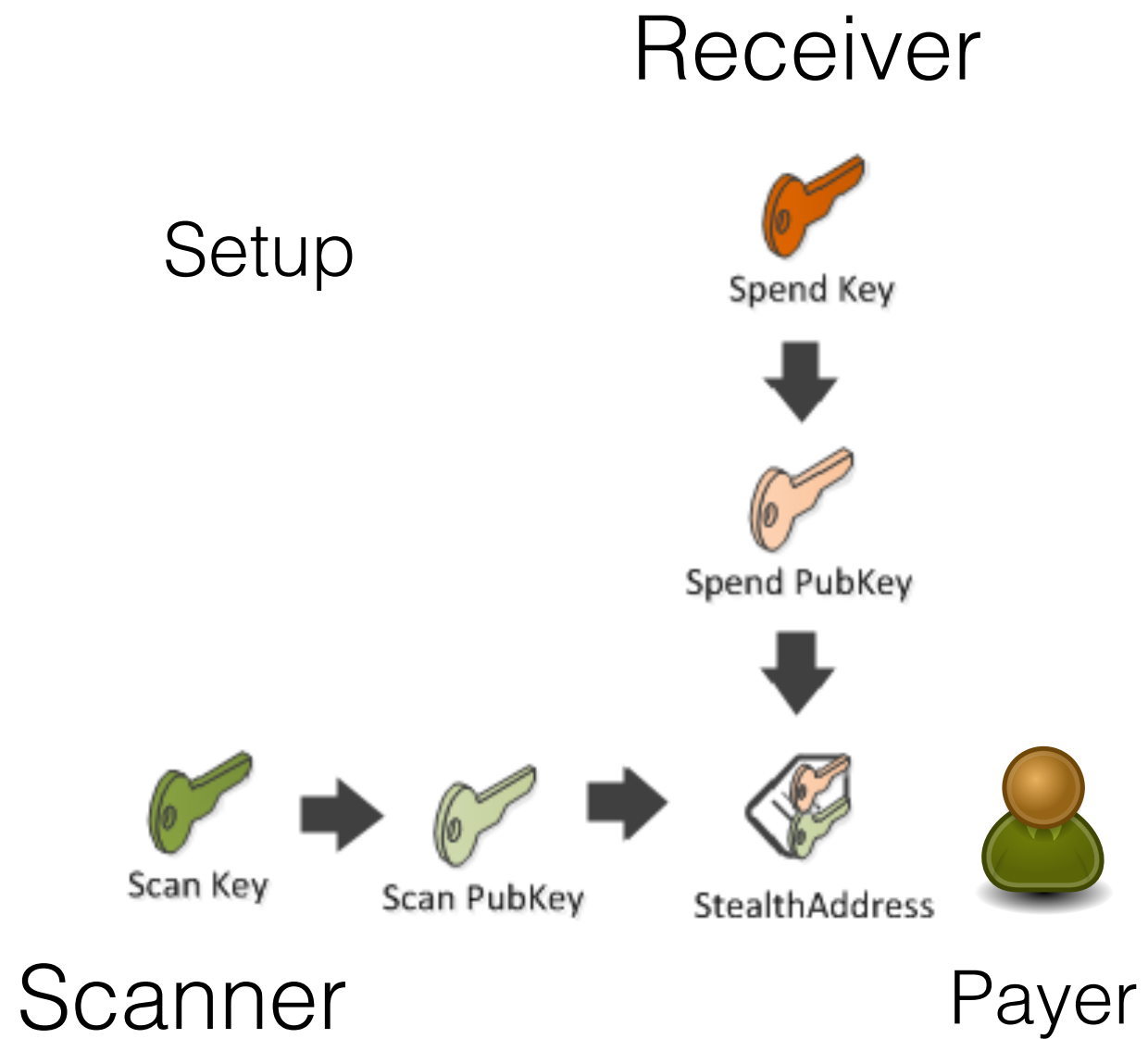
Stealth Addresses 🛡️

Payer ⟵ Stealth address 🛡️ — Receiver

Transaction ⟶

@Alice   @Bob

Adversary
Can't see where
this transaction
is paid to :(

Scanner
Hehe,
I can see

Stealth Addresses - Paying (Dark Wallet)

Stealth Addresses - Paying (Dark Wallet)

Receiver

Setup

Spend Key

Spend PubKey

Scanner

Scan Key → Scan PubKey → StealthAddress

Payer

Stealth Addresses - Paying (Dark Wallet)

Stealth Addresses - Paying (Dark Wallet)

Receiver

Setup

Scanner

Payer

temporary

Pay to address
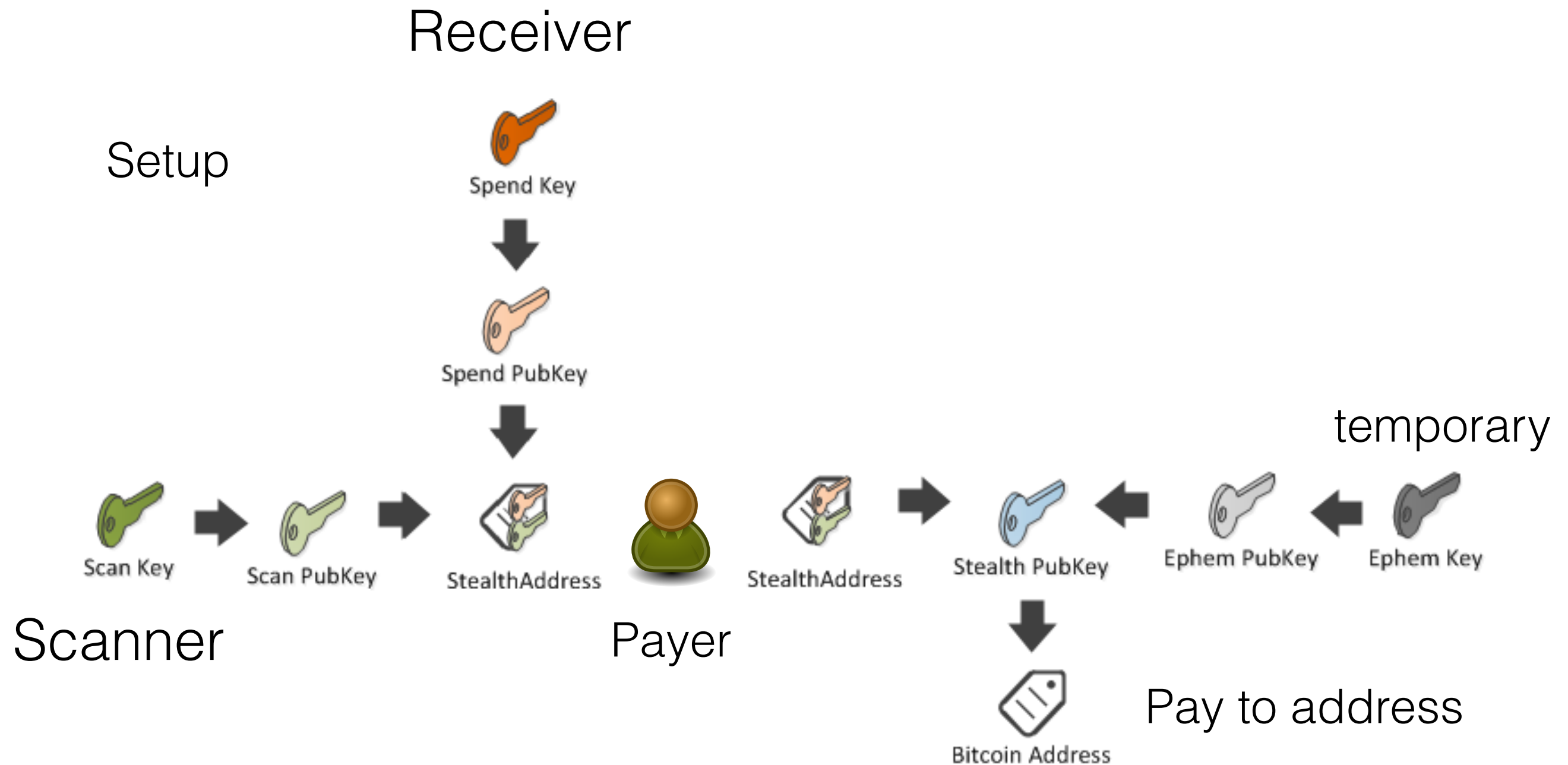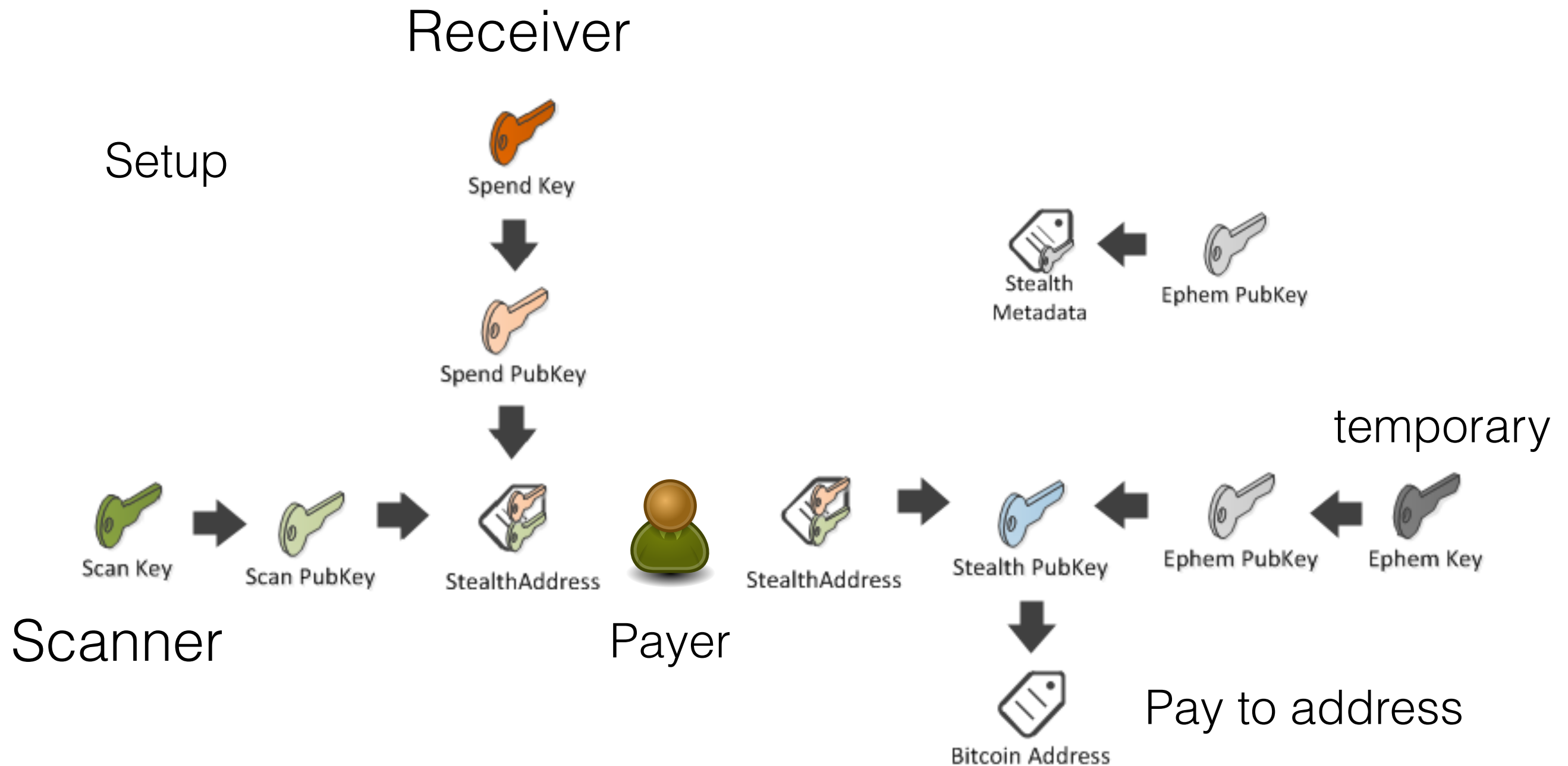
Stealth Addresses - Receiving

StealthAddress

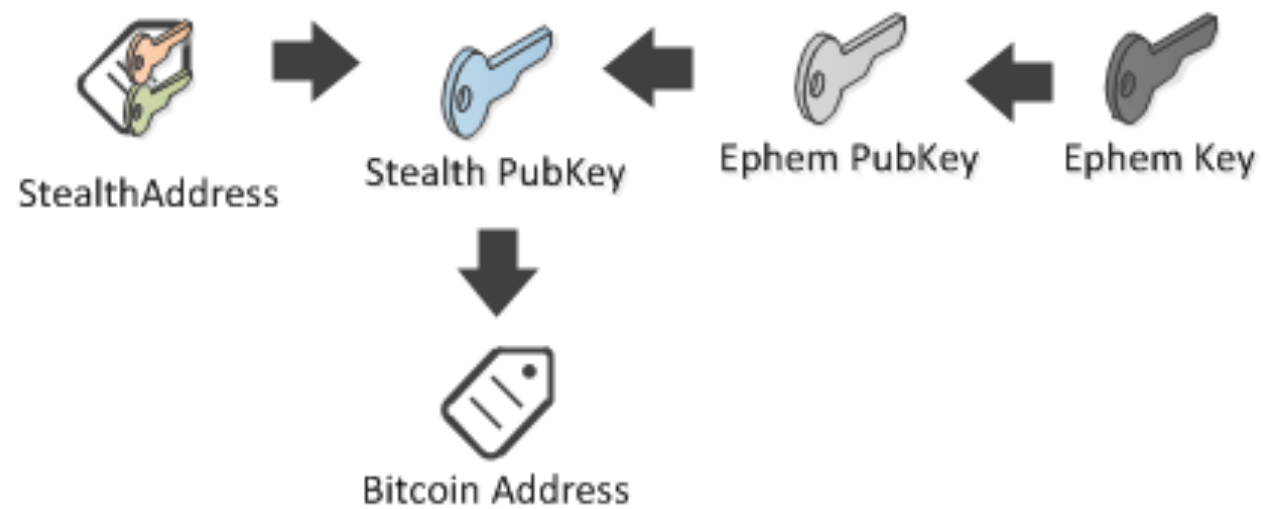Scan Key → Stealth PubKey ← Stealth Metadata

Bitcoin Address
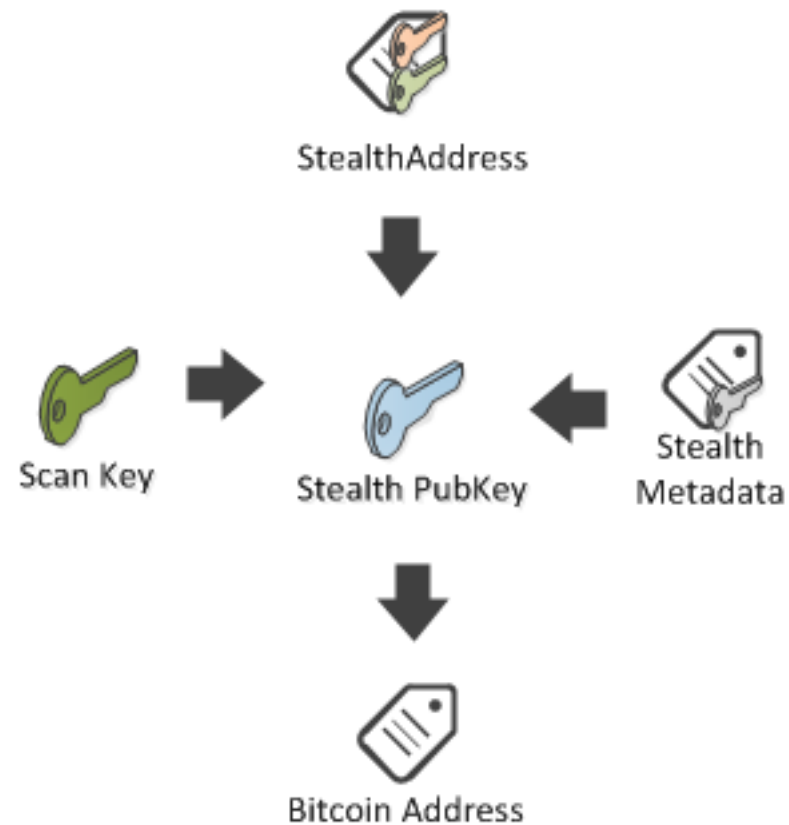
You've received a transaction

Receiver

Stealth Addresses - Spending

Stealth Addresses - Spending

StealthAddress → Stealth PubKey ← Ephem PubKey ← Ephem Key

Stealth PubKey → Bitcoin Address

Stealth Metadata → Stealth Key

Scan Key → Stealth Key ← Spend Key

Receiver
Got the private key
to spend the coins!

Thanks to https://programmingblockchain.gitbook.io/programmingblockchain/key_generation/stealth_address