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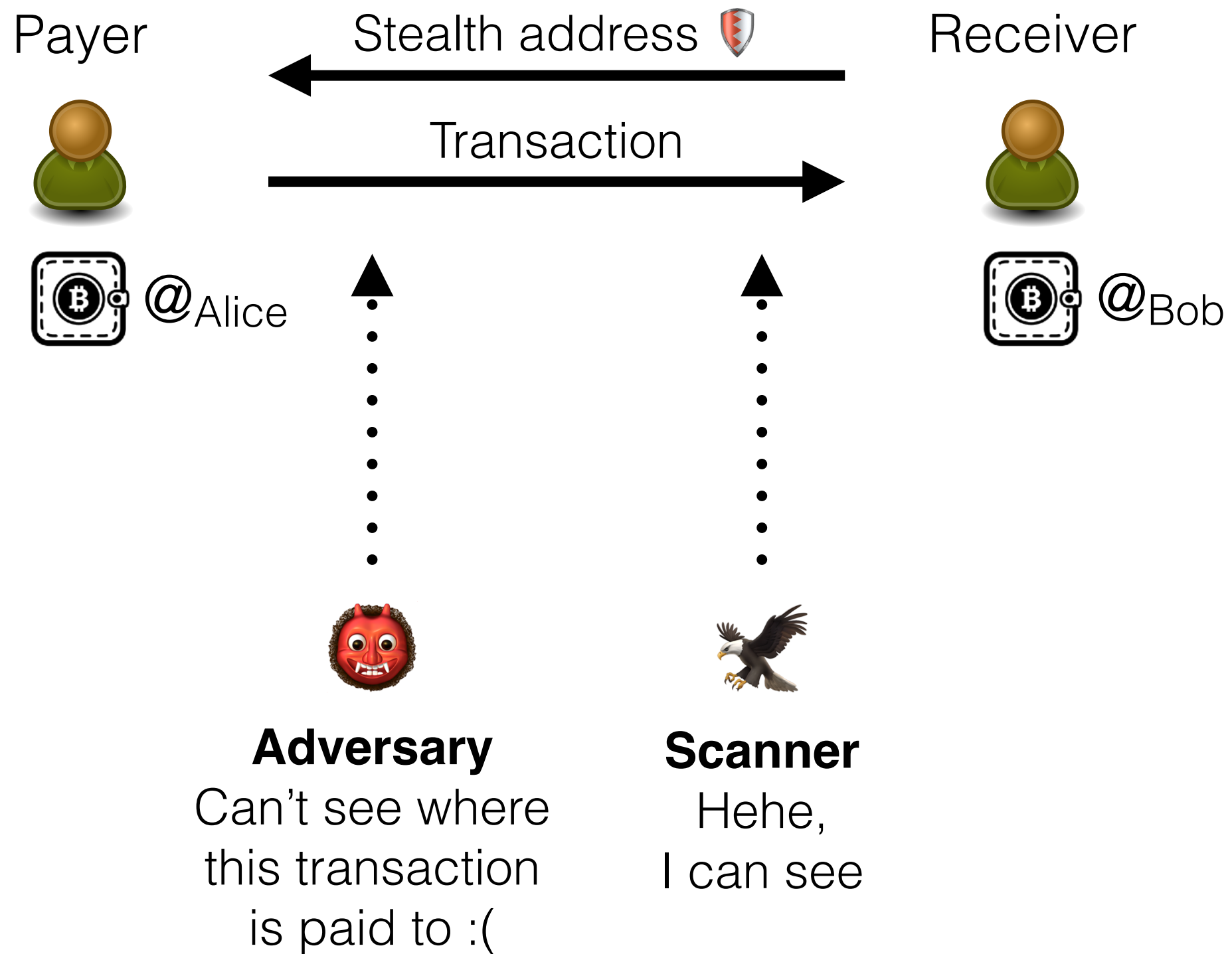
Hierarchical Deterministic (HD) Wallets

```
                          ┌──────────────┐
                          │  Passphrase  │
                          └──────────────┘
                          /       |       \
                         /        |        \
┌────┐ ┌────┐ ┌────┐ ┌────┐ ┌────┐        ┌────┐
│ @1 │ │ @2 │ │ @3 │ │ @4 │ │ @5 │  ...   │ @n │
└────┘ └────┘ └────┘ └────┘ └────┘        └────┘
```
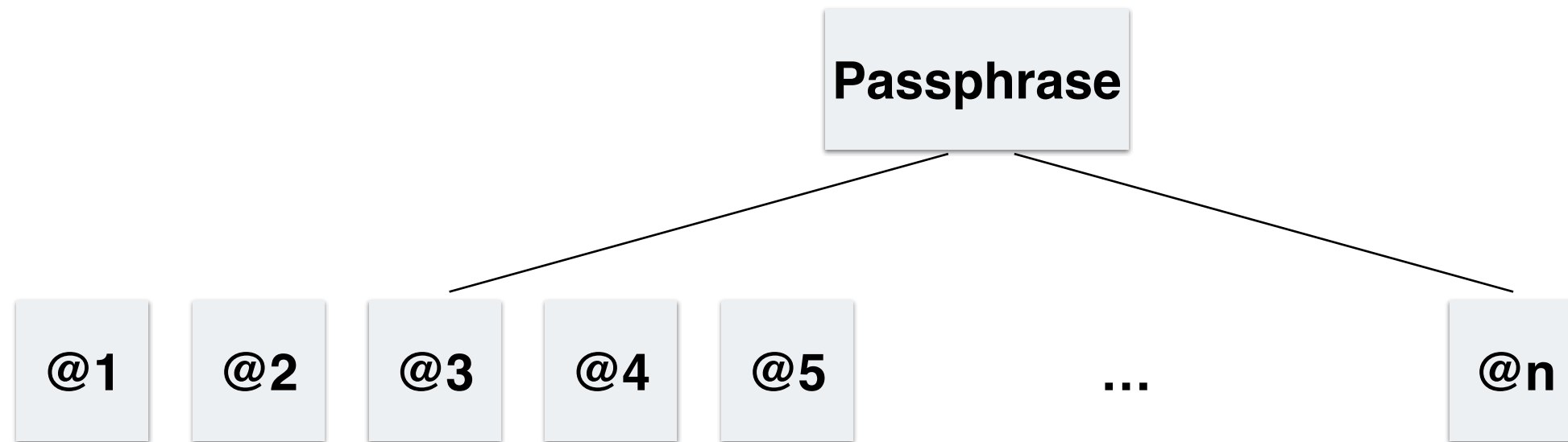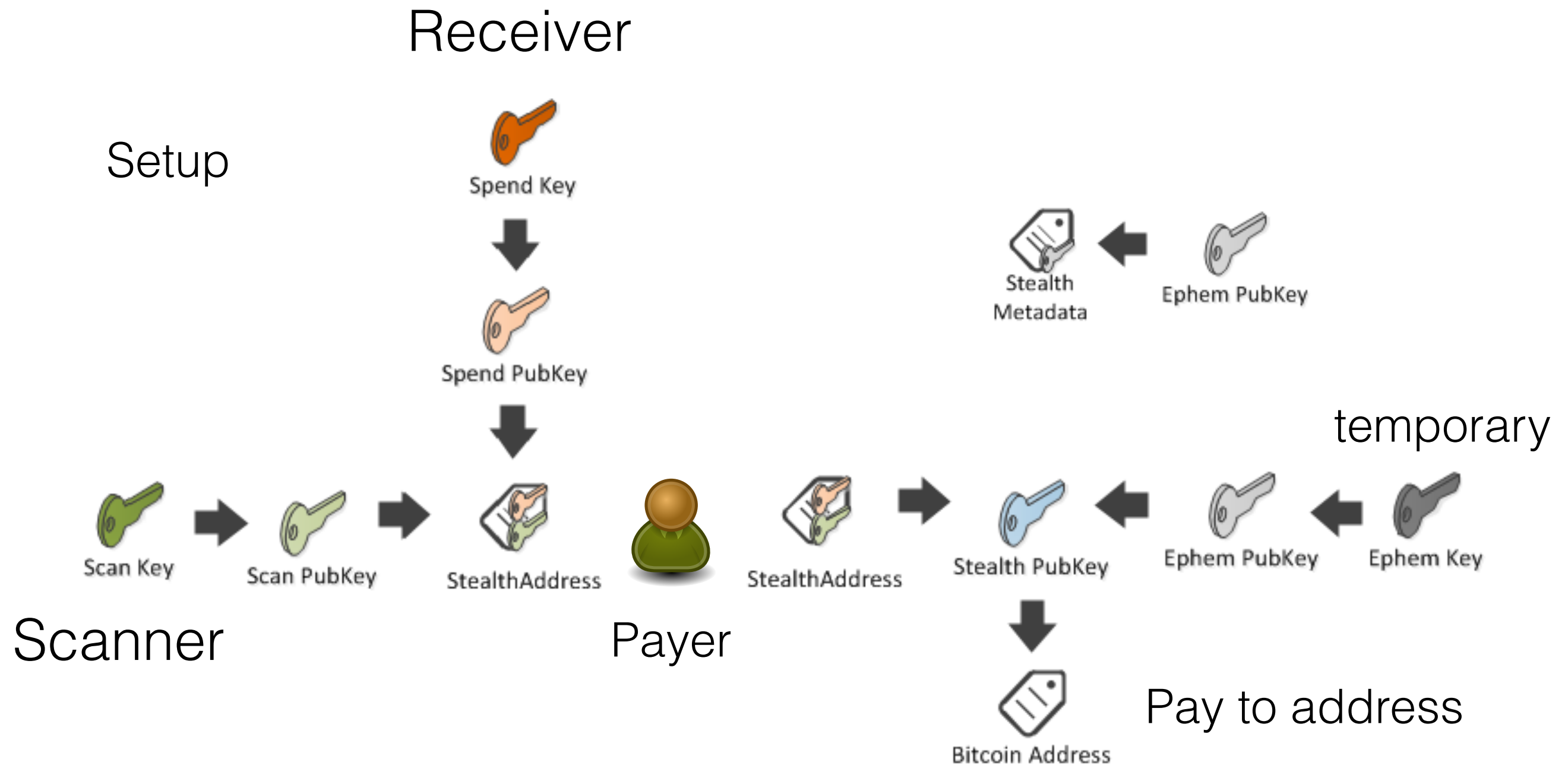
- Addresses derived from the same key

- From one address cannot derive the other addresses

- Used by the majority of Bitcoin/Ethereum wallets today
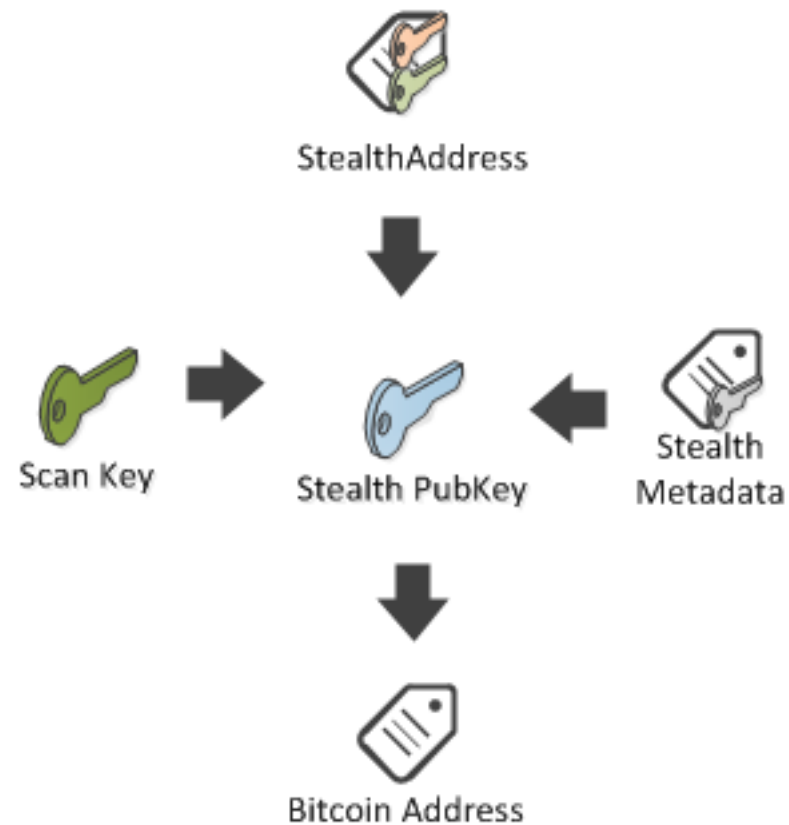
- A form of stealth addresses

Stealth Addresses 🛡️

Payer

Stealth address 🛡️

Transaction

Receiver

@$_{Alice}$

@$_{Bob}$

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

Scanner
Hehe,
I can see

Stealth Addresses - Paying (Dark Wallet)

Receiver

Setup

Spend Key

Spend PubKey

Stealth Metadata ← Ephem PubKey

temporary

Scan Key → Scan PubKey → StealthAddress

Scanner

Payer

StealthAddress → Stealth PubKey ← Ephem PubKey ← Ephem Key

Bitcoin Address

Pay to address

Stealth Addresses - Receiving

StealthAddress

Scan Key → Stealth PubKey ← Stealth Metadata

Bitcoin Address

You've received a transaction

Receiver

Stealth Addresses - Spending

Receiver
Got the private key
to spend the coins!