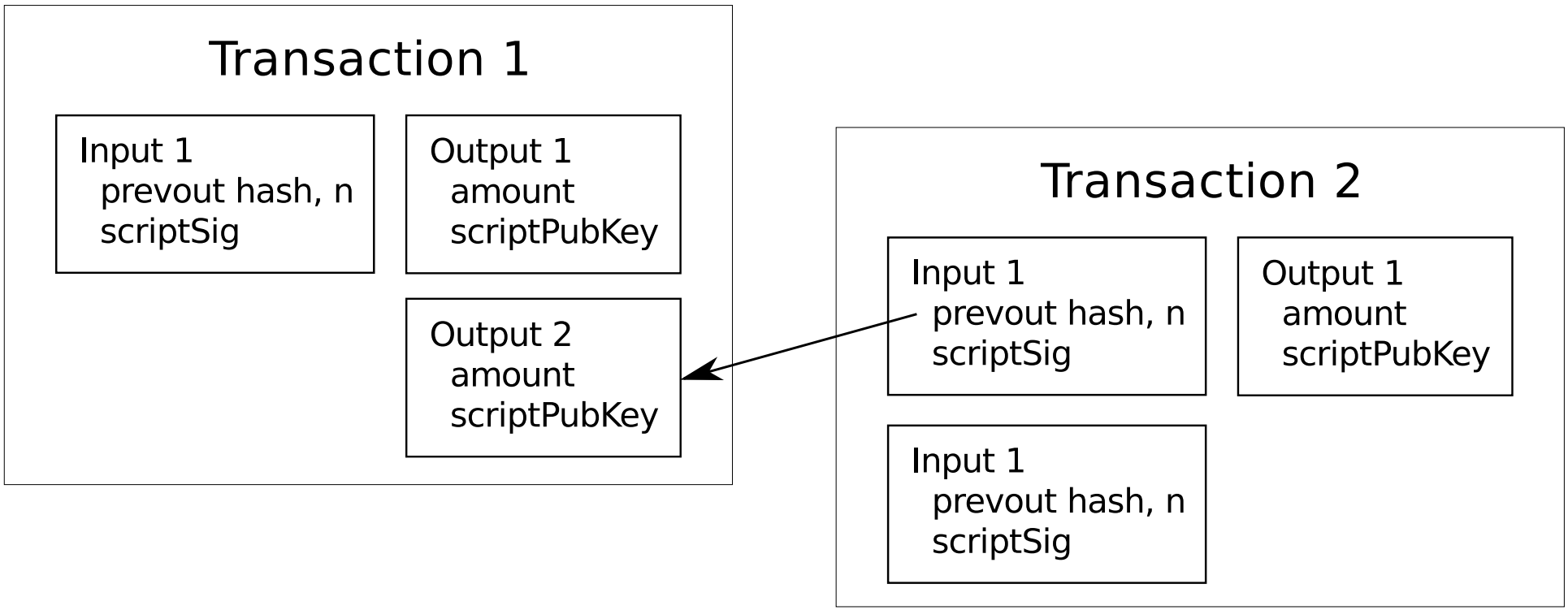
Bitcoin Wallet

January 24, 2018

Simplest Wallet: Set of keypairs

- Collection of (public key, private key) pairs.
- Anyone with BTC and one of your public keys can set aside money for you, creating transaction output, which you can spend in future transactions signed by your private key.

Bitcoin Transactions



scriptPubkey ≈ public key + conditions

- scriptPubKey is script determine conditions txout can be spent: what signatures and other data needs to be provided
- Standard scriptPubKey allows txout to be spent given valid signature from public key with specified hash.
- Can have other conditions: multisig, hash preimage

Address = scriptPubKey + metadata

- No generic address format, not possible to write an address for every scriptPubKey, only standard scriptPubKeys.
- Base58, Bech32 formats encode other metadata, too: mainnet/testnet bits, checksums.

Keypairs ↔ Scripts ↔ Addresses

How many... (0/1/2/3+/∞)

- ...different address strings can be used to represent a given scriptPubKey?
  - 0 if nonstandard or 2 if standard (different addresses mainnet testnet)
- ...different scriptPubKeys may be used to send to funds to a given address?
  - 1
- ...different scriptPubKeys may be redeemable with a given keypair
  - ∞ nonstandard scriptPubKeys, plus many standard ones (P2PK, P2PKH, P2WPKH, variants embedded in P2SH, variants compressed / uncompressed)
- ...keypairs can be used to redeem a scriptPubKey
  - 1 for normal scriptPubKey, any number for weird pub keys (multisig, etc)

Keypairs ↔ Scripts ↔ Addresses

How many... (0/1/2/3+/∞)

- ...different address strings can be used to represent a given scriptPubKey?
  - 0 if nonstandard or 2 if standard (different addresses mainnet testnet)
- ...different scriptPubKeys may be used to send to funds to a given address?
  - 1
- ...different scriptPubKeys may be redeemable with a given keypair
  - ∞ nonstandard scriptPubKeys, plus many standard ones (P2PK, P2PKH, P2WPKH, variants embedded in P2SH, variants compressed / uncompressed)
- ...keypairs can be used to redeem a scriptPubKey
  - 1 for normal scriptPubKey, any number for weird pub keys (multisig, etc)

Keypairs ↔ Scripts ↔ Addresses

How many... (0/1/2/3+/∞)

- ...different address strings can be used to represent a given scriptPubKey?
  - 0 if nonstandard or 2 if standard (different addresses mainnet testnet)
- ...different scriptPubKeys may be used to send to funds to a given address?
  - 1
- ...different scriptPubKeys may be redeemable with a given keypair
  - ∞ nonstandard scriptPubKeys, plus many standard ones (P2PK, P2PKH, P2WPKH, variants embedded in P2SH, variants compressed / uncompressed)
- ...keypairs can be used to redeem a scriptPubKey
  - 1 for normal scriptPubKey, any number for weird pub keys (multisig, etc)

Keypairs $\leftrightarrow$ Scripts $\leftrightarrow$ Addresses

How many... (0/1/2/3+/∞)

- ...different address strings can be used to represent a given scriptPubKey?
  - 0 if nonstandard or 2 if standard (different addresses mainnet testnet)
- ...different scriptPubKeys may be used to send to funds to a given address?
  - 1
- ...different scriptPubKeys may be redeemable with a given keypair
  - ∞ nonstandard scriptPubKeys, plus many standard ones (P2PK, P2PKH, P2WPKH, variants embedded in P2SH, variants compressed / uncompressed)
- ...keypairs can be used to redeem a scriptPubKey
  - 1 for normal scriptPubKey, any number for weird pub keys (multisig, etc)

Keypairs ↔ Scripts ↔ Addresses

How many... (0/1/2/3+/∞)

- ...different address strings can be used to represent a given scriptPubKey?
  - 0 if nonstandard or 2 if standard (different addresses mainnet testnet)
- ...different scriptPubKeys may be used to send to funds to a given address?
  - 1
- ...different scriptPubKeys may be redeemable with a given keypair
  - ∞ nonstandard scriptPubKeys, plus many standard ones (P2PK, P2PKH, P2WPKH, variants embedded in P2SH, variants compressed / uncompressed)
- ...keypairs can be used to redeem a scriptPubKey
  - 1 for normal scriptPubKey, any number for weird pub keys (multisig, etc)

Complications

- Keypools
- HD keys
- Watch only keys

Schema

- ddd