CodeChain Core & Use cases

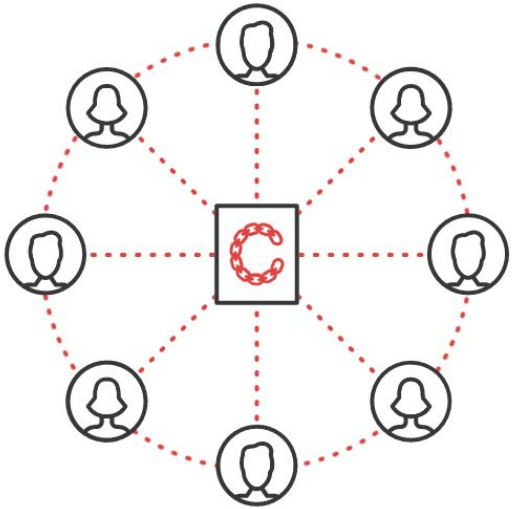
2018-06-08

About US

Kodebox is a blockchain technology company on a mission to create and enable a smarter asset management system

KODEBOX

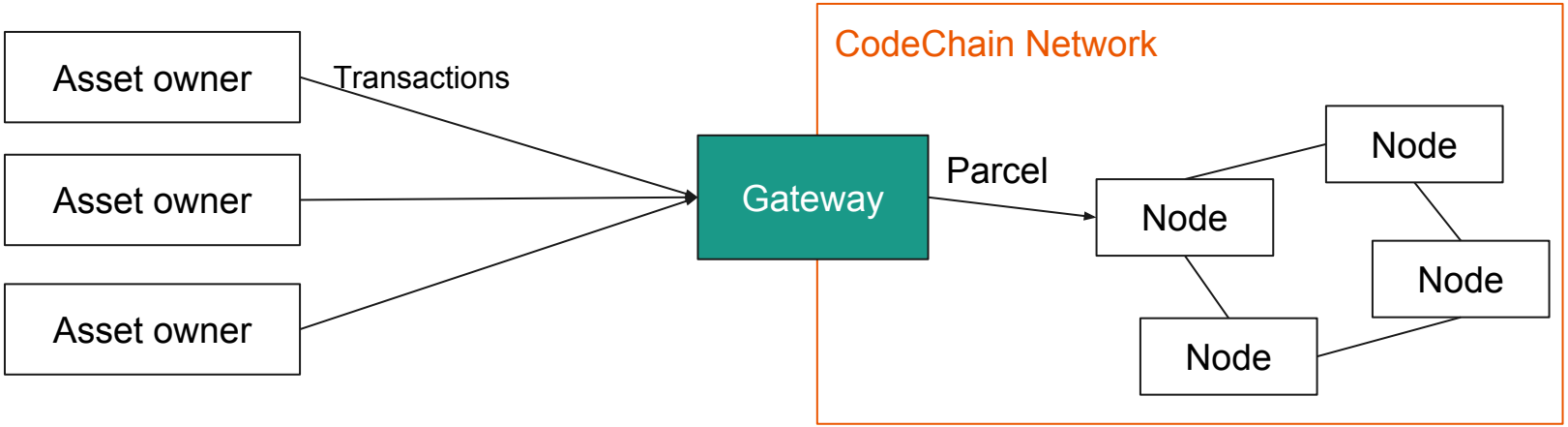
CodeChain



CodeChain is a programmable open source blockchain technology optimal for developing and customizing multi-asset management systems

User doesn’t pay the fee

User doesn't pay the fee



Parcel

```rust
pub struct Parcel {
    pub nonce: U256,
    pub fee: U256,
    pub transactions: Vec<Transaction>,
    pub network_id: u64,
}

pub enum Transaction {
    AssetTransfer {
        network_id: u64,
        inputs: Vec<AssetTransferInput>,
        outputs: Vec<AssetTransferOutput>,
        nonce: u64,
    },
    AssetMint {
        metadata: String,
        lock_script_hash: H256,
        parameters: Vec<Bytes>,
        amount: Option<u64>,
        registrar: Option<Address>,
        nonce: u64,
    }
}
```

- Fee determines priority
- Minimum fee exists
- *nonce* prevents replay attack
- Sender is derived from the signature

Platform Account

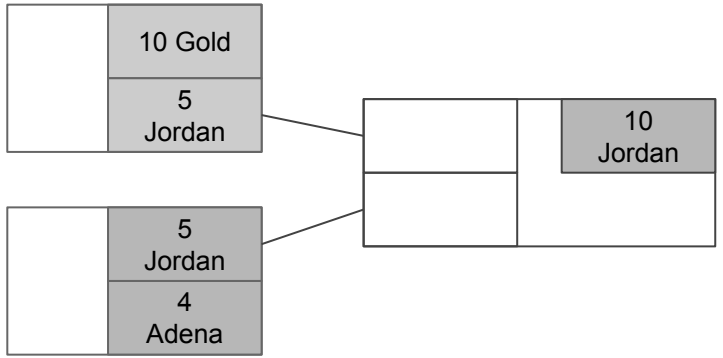
- Holds platform coins (CCC) used to pay for transaction fees
- Minimum deposit of CCC is required to activate an account
- Decoupled from asset ownership

Who can unlock the script owns the Asset

Asset Transfer

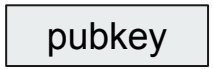
```rust
pub struct AssetTransferInput {
    pub prev_out: AssetOutPoint,
    pub lock_script: Bytes,
    pub unlock_script: Bytes,
}

pub struct AssetOutPoint {
    pub transaction_hash: H256,
    pub index: usize,
    pub asset_type: H256,
    pub amount: u64,
}
```

```rust
pub struct AssetTransferOutput {
    pub lock_script_hash : H256,
    pub parameters: Vec<Bytes>,
    pub asset_type: H256,
    pub amount: u64,
}
```



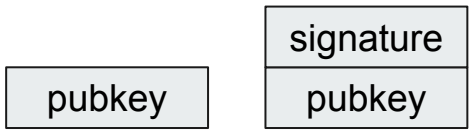
Pay to pub key

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig



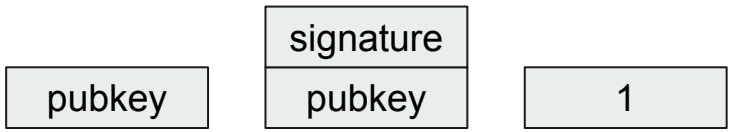
Pay to pub key

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig



Pay to pub key

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig



Pay to pub key

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig

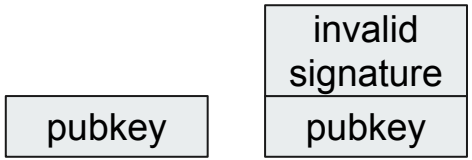
Burn 1/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn

pubkey

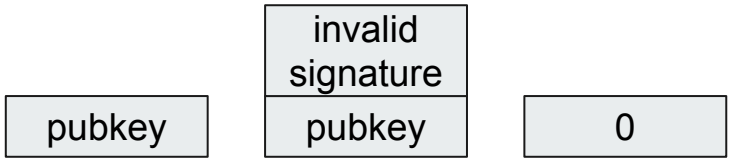
Burn 1/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn



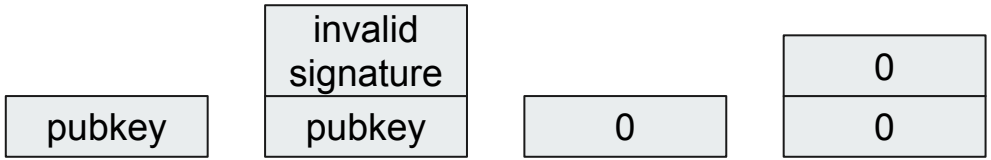
Burn 1/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn



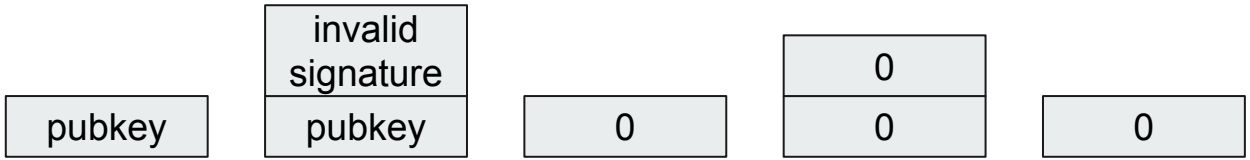
Burn 1/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn



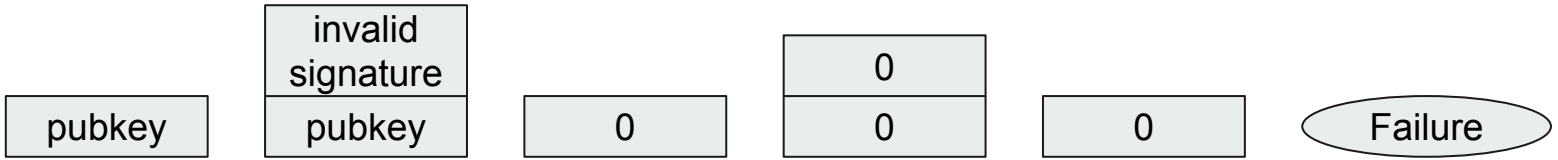
Burn 1/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn



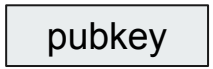
Burn 1/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn



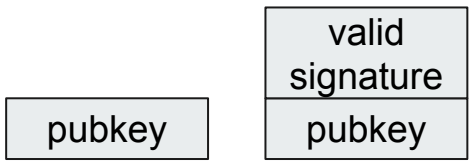
Burn 2/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn



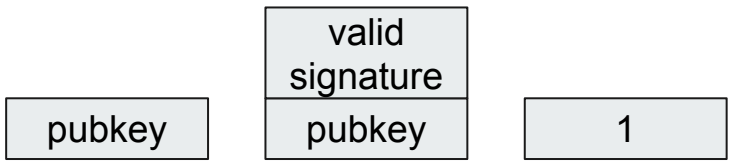
Burn 2/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn



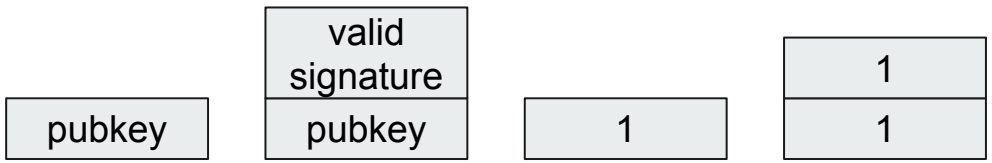
Burn 2/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn



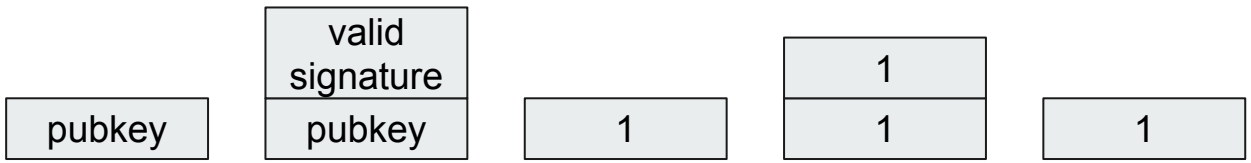
Burn 2/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn



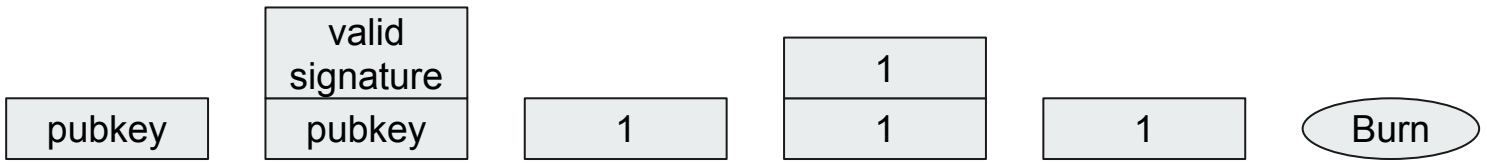
Burn 2/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn



Burn 2/2

Unlock Script: Push <signature>
Parameters: <pubkey>
Lock Script: ChkSig Dup Jz 2 Burn

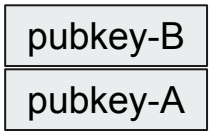


Conditional signature 1/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

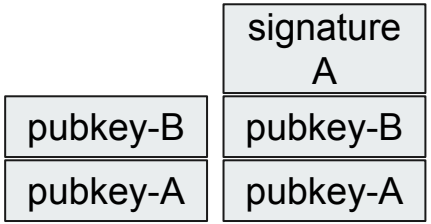


Conditional signature 1/3

Unlock Script: Push <signature>

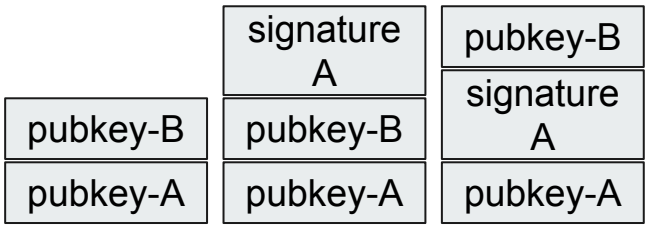
Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop



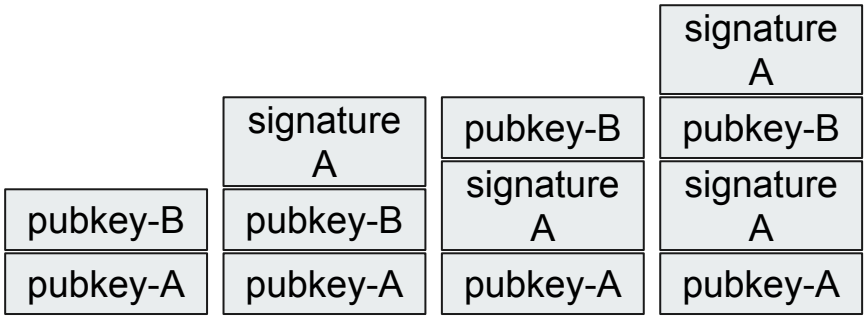
Conditional signature 1/3

Unlock Script: Push <signature>
Parameters: <pubkey-A> <pubkey-B>
Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop



Conditional signature 1/3

Unlock Script: Push <signature>
Parameters: <pubkey-A> <pubkey-B>
Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

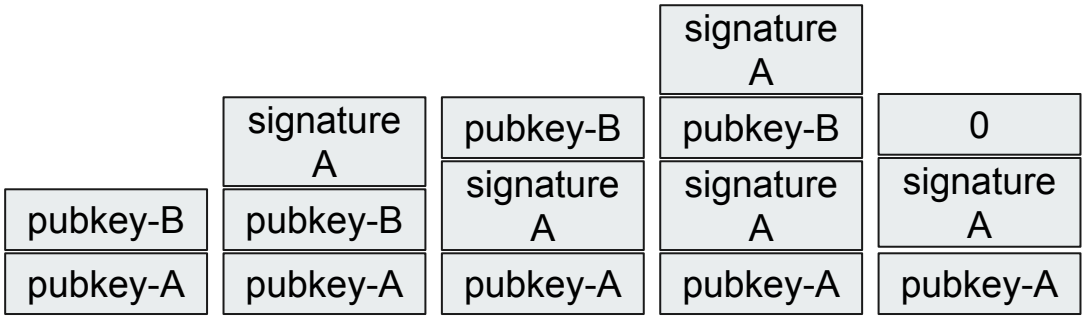


Conditional signature 1/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

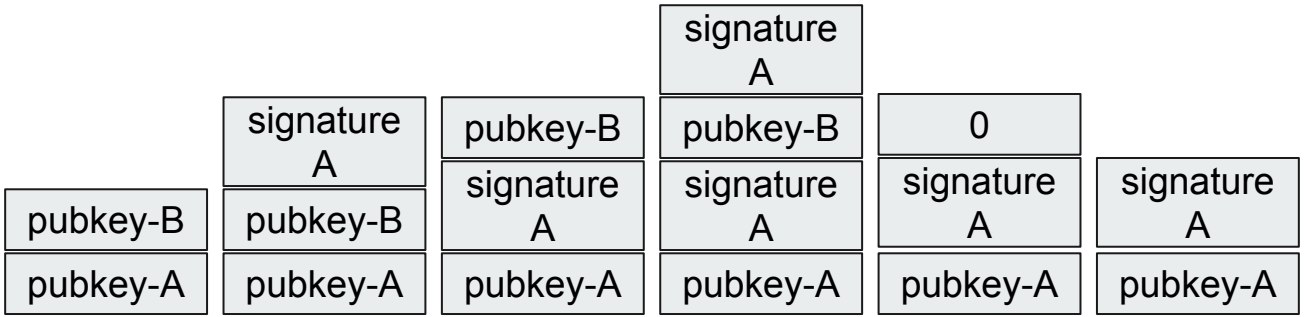


Conditional signature 1/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

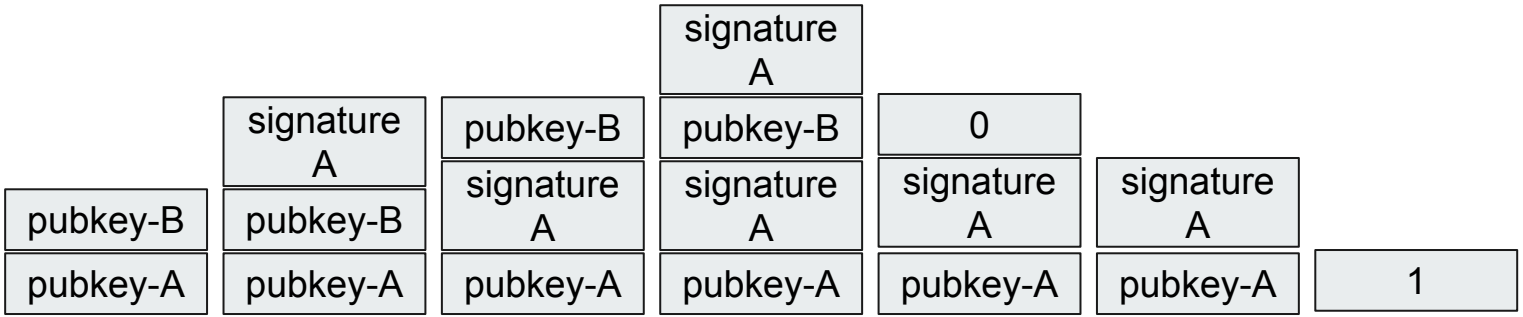


Conditional signature 1/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

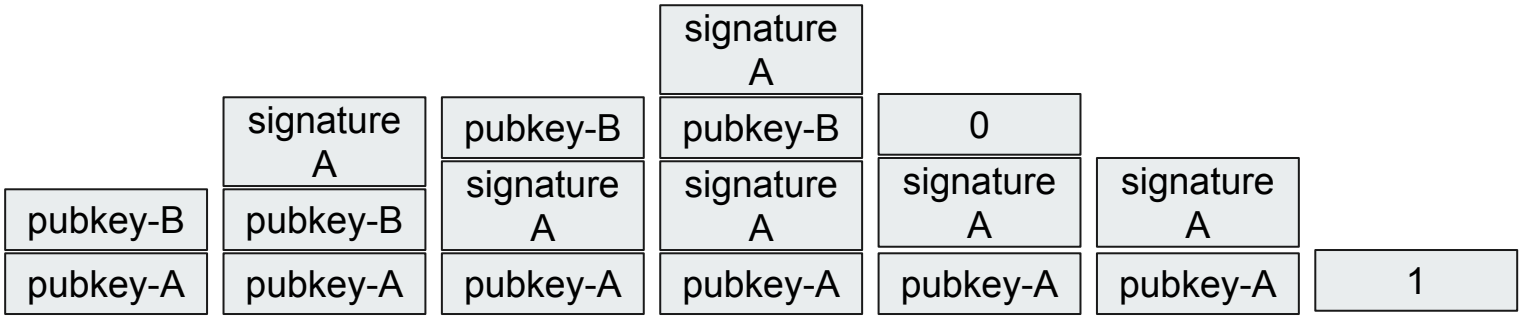


Conditional signature 1/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

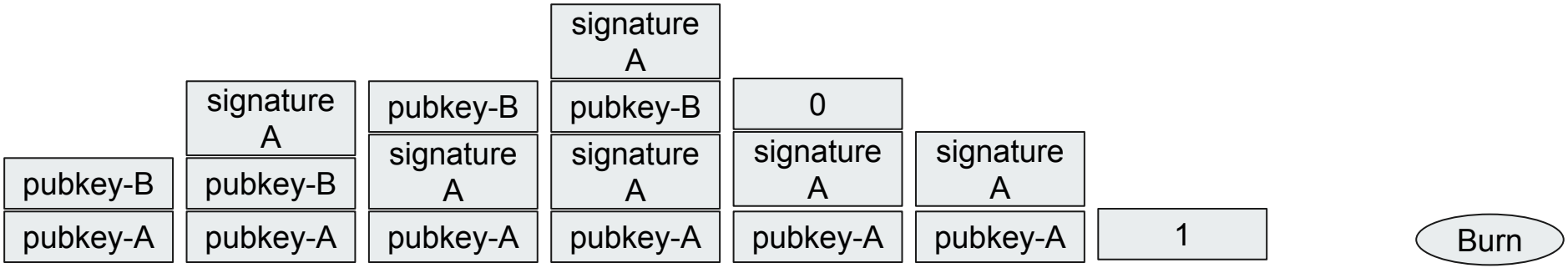


Conditional signature 1/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

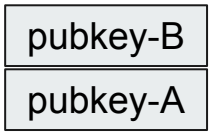


Conditional signature 2/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

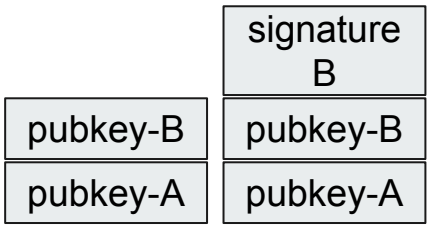


Conditional signature 2/3

Unlock Script: Push <signature>

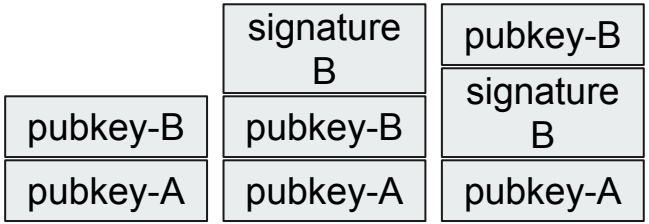
Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop



Conditional signature 2/3

Unlock Script: Push <signature>
Parameters: <pubkey-A> <pubkey-B>
Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

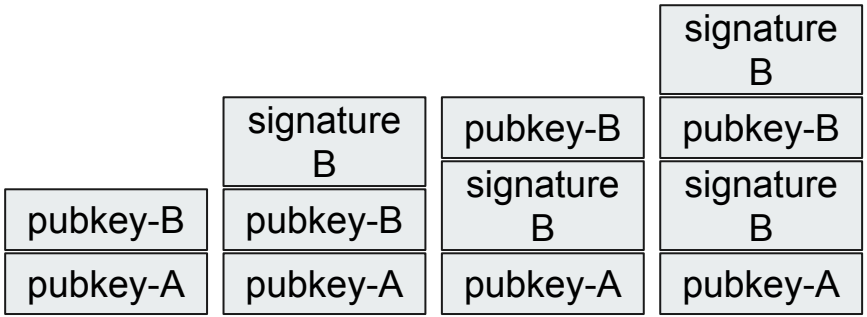


Conditional signature 2/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

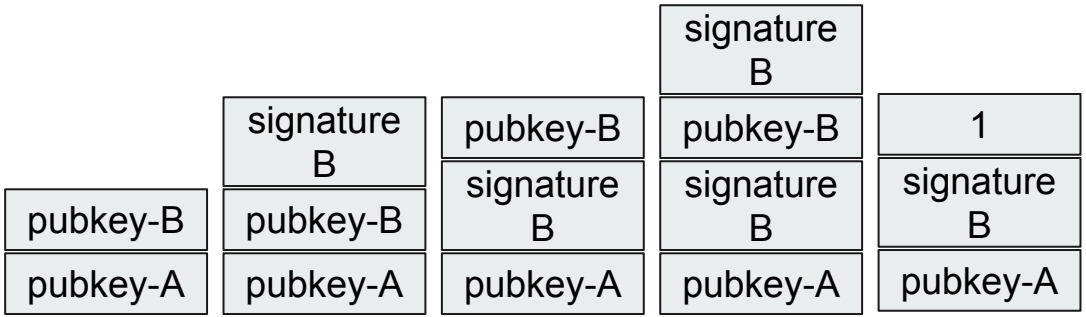


Conditional signature 2/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

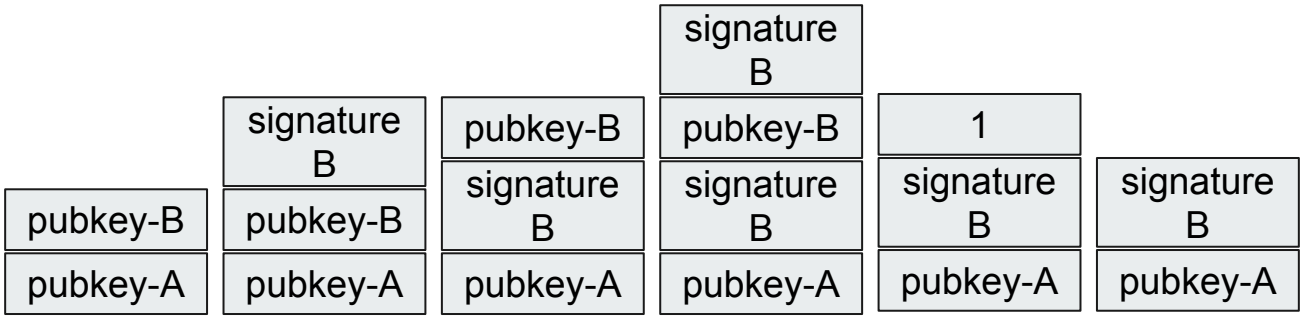


Conditional signature 2/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

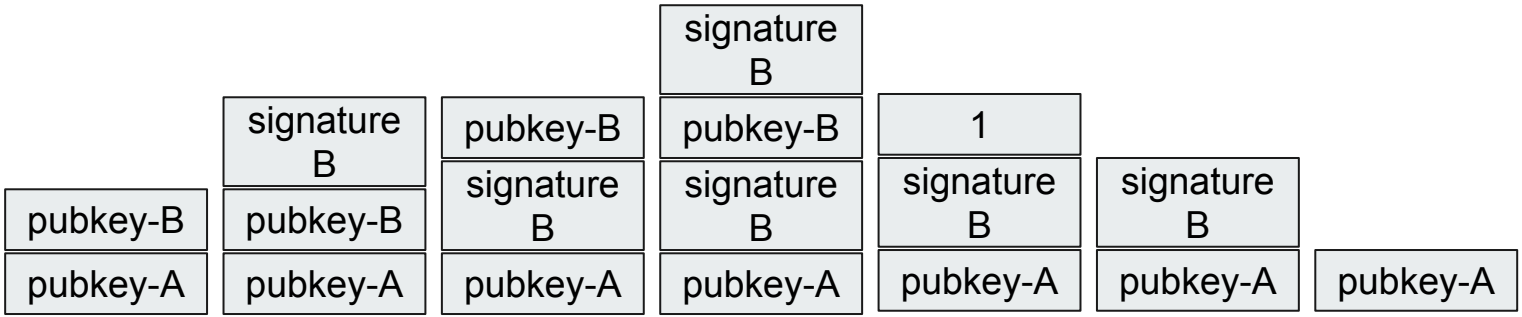


Conditional signature 2/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

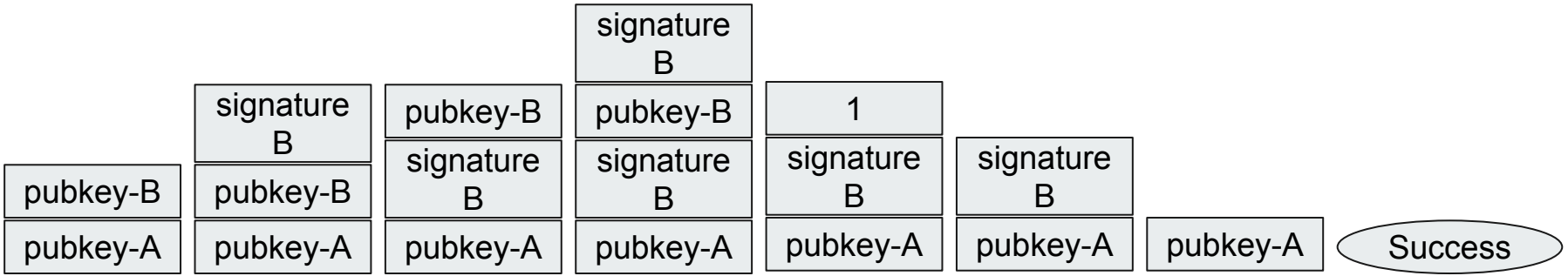


Conditional signature 2/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop



Conditional signature 3/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

pubkey-B

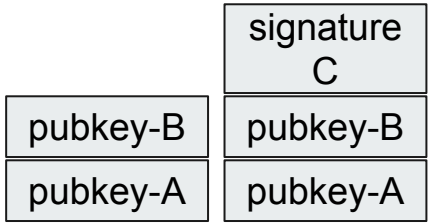
pubkey-A

Conditional signature 3/3

Unlock Script: Push <signature>

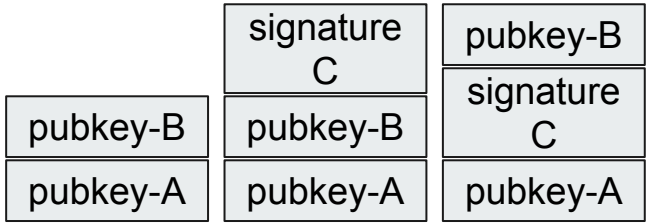
Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop



Conditional signature 3/3

Unlock Script: Push <signature>
Parameters: <pubkey-A> <pubkey-B>
Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

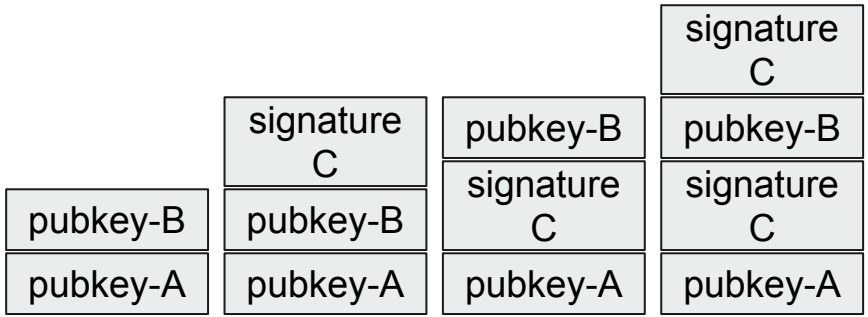


Conditional signature 3/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop



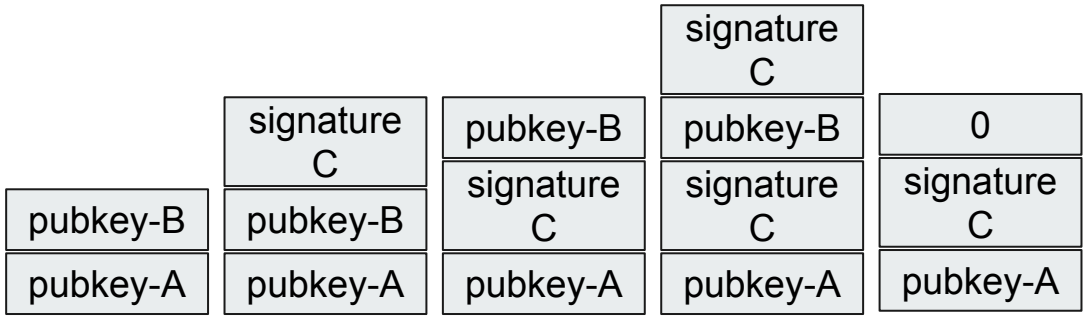
KODEBOX

Conditional signature 3/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

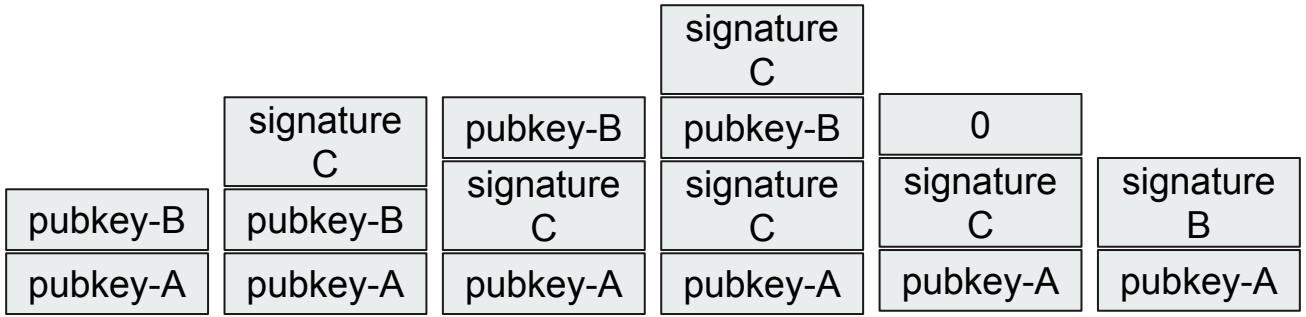


Conditional signature 3/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop



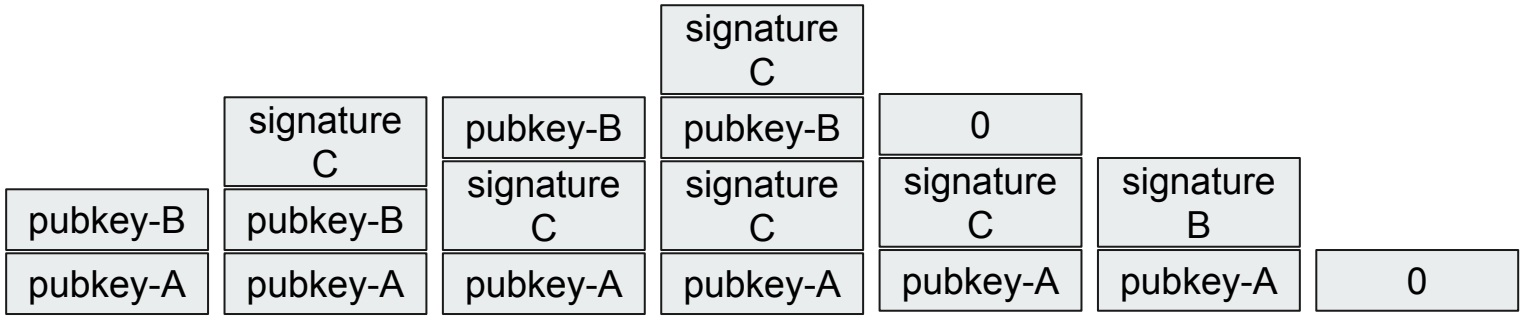
KODEBOX

Conditional signature 3/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

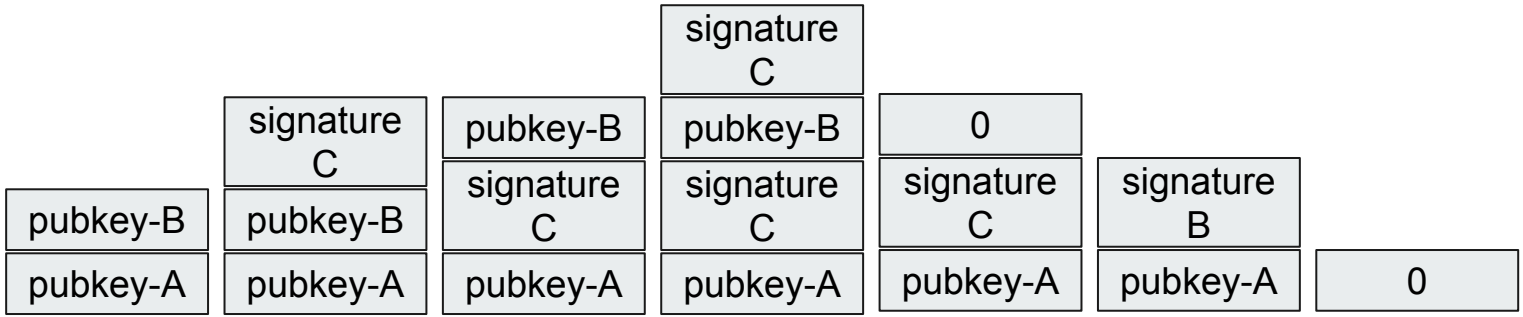


Conditional signature 3/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop

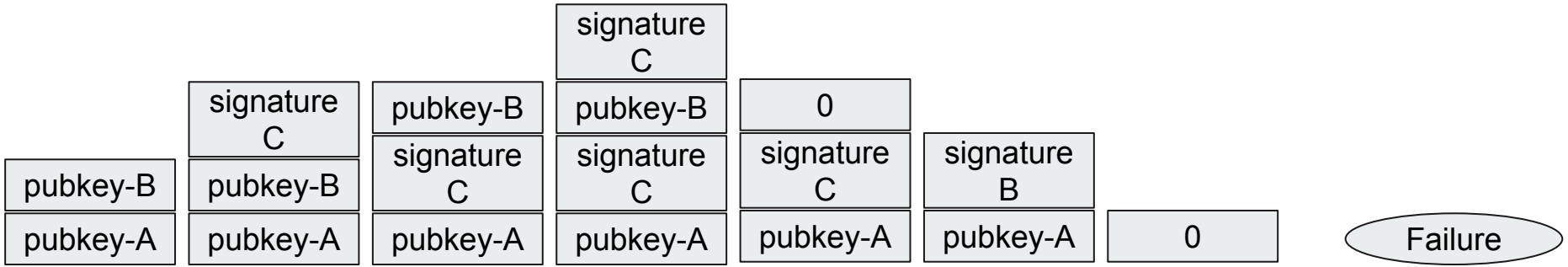


Conditional signature 3/3

Unlock Script: Push <signature>

Parameters: <pubkey-A> <pubkey-B>

Lock Script: Swap Copy 1 ChkSig Jnz 4 ChkSig Jz 2 Burn Pop



KODEBOX

Thank You

Home
http://codechain.io/

Blog
https://medium.com/codechain/

Facebook Page
https://www.facebook.com/codechain/

Twitter
https://twitter.com/codechain_io