Cryptocurrencies & Security on the Blockchain

Bitcoin Transactions, In Depth

Prof. Tom Austin
San José State University

GRADED Reading Summary

Before next class, read Bonneau et al.'s "*SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*".

Be prepared to discuss next class.

http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf

Transaction Lifecycle

1. Origination: creation of a transaction.
   - All information is public.
2. Signed (one or more parties) to authorize spending.
3. Validated and propagated by nodes in network.
   - Avoid propagating invalid transaction.
4. Verified by mining node and included in block.

Transaction

- Amount of BTC, in satoshis.
  - Satoshi = 0.00000001 BTC, smallest unit of BTC.
- Locking script.
  - Terms for funds to be released.
  - Spending conditions.
    - AKA *encumbrences*.

Transaction inputs and outputs

- Mapping of inputs to outputs forms *transaction chains*.
- Inputs – stored on blockchain.
- Outputs (UTXOs) stored in RAM.

Transaction input

- Pointer to UTXO
- Unlocking script matches conditions of UTXO's locking script
- Orphan transactions
  - Transactions whose UTXO has not yet been seen by the miner.
  - Max size to prevent DoS attacks

Bitcoin "Script" Language

- Forth-like
  - Reverse-Polish notation
  - Stack based
- Lock: `scriptPubKey`
- Unlock: `scriptSig`
- https://en.bitcoin.it/wiki/Script

Sample Transaction Output

```
"vout": [
   { "value": 0.01500000,
     "scriptPubKey": "OP_DUP OP_HASH160
         ab6802… OP_EQUALVERIFY
         OP_CHECKSIG" },
   { "value": 0.08450000,
     "scriptPubKey": "OP_DUP OP_HASH160
         7f9b1a… OP_EQUALVERIFY
         OP_CHECKSIG" },
]
```

Script Limitations

- No loops.
- No complex control flow.
- Not Turing complete.
- No division.

Sample Script

```
2 7 OP_ADD 3 OP_SUB 1 OP_ADD 7 OP_EQUAL
```

(in-class)

Standard Transactions

- Safe "templates" for transactions.
- Many miners will ignore non-standard transactions.
- Non-standard transactions can still be accepted.
  - Find a miner who will accept it.

Standard Transactions

- Pay-to-public-key
- Pay-to-public-key-hash (P2PKH)
- Multi signature
  - Multiple signatures required.
  - M-of-N schemes often used.
- Pay-so-script-hash (P2SH)
- Data output

Pay-to-public-key and P2PKH

- Pay-to-public-key:
  - Unlock by presenting public key and signature
  - Public key is large
  - Allowed, but largely fading from use
- P2PKH
  - Instead uses the *hash* of the key, in hex format
  - Otherwise, works the same way

Sample P2PKH Script

```
<sig> <PubK> DUP HASH160 <PubKHash>
                    EQUALVERIFY CHECKSIG
```

(in-class)

Data Output

- Store data on the blockchain in an *unspendable* UTXO.
  - Controversial, since UTXOs are stored in RAM.
  - Blockchain bloat.
- OP_RETURN.
  - Special opcode that produces a *provably* unspendable UTXO.
    - UTXO does not need to be stored in RAM.

P2SH

- Pay to a script matching a hash.
- Creates reusable scripts.

Blockexplorer.com

(in-class)