Bitcoin Transactions

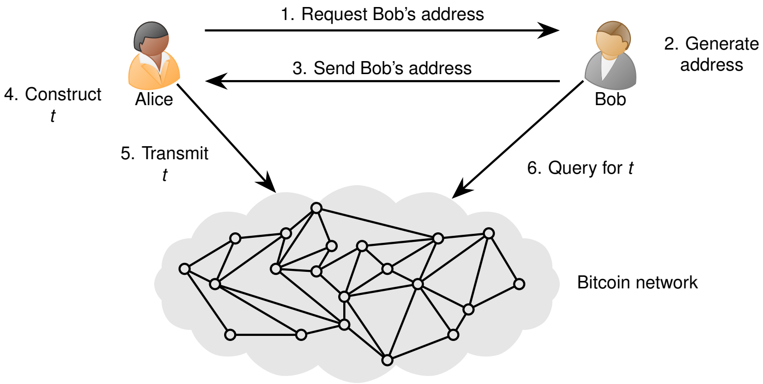
Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

August 3, 2018

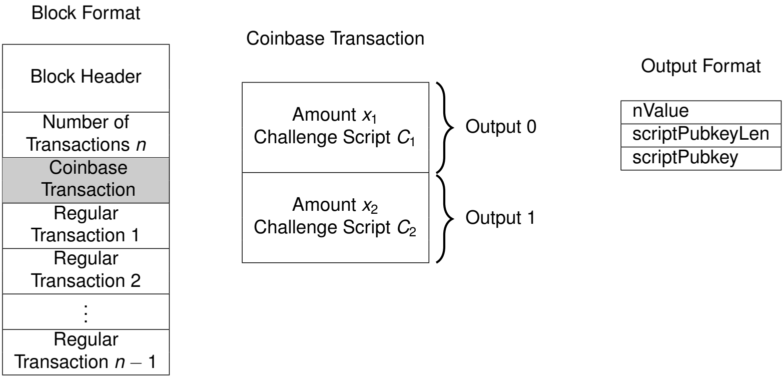
Bitcoin Transactions

Bitcoin Payment Workflow



- Merchant Bob shares address out of band (not using Bitcoin P2P)
- Customer Alice broadcasts transaction *t* which pays the address
- Miners collect broadcasted transactions into a candidate block
- One of the candidate blocks containing *t* is mined
- Merchant waits for confirmations on *t* before providing goods

Coinbase Transaction Format



Block Format

Block Header

Number of Transactions n

Coinbase Transaction

Regular Transaction 1

Regular Transaction 2

⋮

Regular Transaction $n-1$

Coinbase Transaction

Amount x_1
Challenge Script C_1

Output 0

Amount x_2
Challenge Script C_2

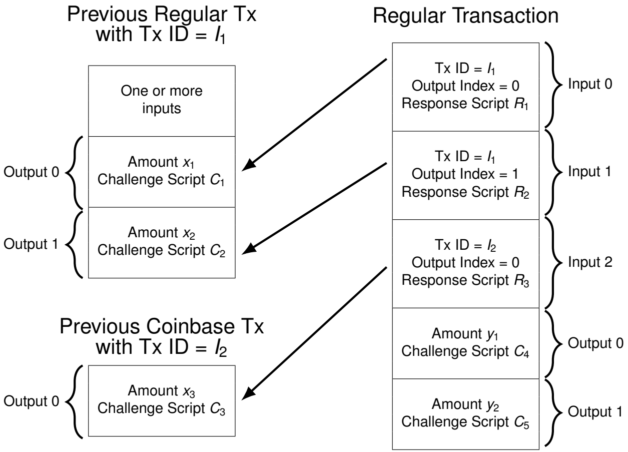
Output 1

Output Format

nValue
scriptPubkeyLen
scriptPubkey

- nValue contains number of satoshis locked in output
    - 1 Bitcoin = 10^8 satoshis
- scriptPubkey contains the challenge script
- scriptPubkeyLen contains byte length of challenge script

Regular Transaction Format



Previous Regular Tx with Tx ID = I_1

One or more inputs

Output 0: Amount x_1 Challenge Script C_1

Output 1: Amount x_2 Challenge Script C_2

Previous Coinbase Tx with Tx ID = I_2

Output 0: Amount x_3 Challenge Script C_3

Regular Transaction

Input 0: Tx ID = I_1 Output Index = 0 Response Script R_1

Input 1: Tx ID = I_1 Output Index = 1 Response Script R_2

Input 2: Tx ID = I_2 Output Index = 0 Response Script R_3

Output 0: Amount y_1 Challenge Script C_4

Output 1: Amount y_2 Challenge Script C_5

Input Format

hash
n
scriptSigLen
scriptSig
nSequence

Output Format

nValue
scriptPubkeyLen
scriptPubkey

- hash and n identify output being unlocked
- scriptSig contains the response script

References

- Chapter 5 of *An Introduction to Bitcoin*, S. Vijayakumaran, `www.ee.iitb.ac.in/~sarva/bitcoin.html`