UTXO vs Account Balance

Some Notes - Working on

UTXO - Used in BTC

- Inspired by Cash System: Tx = Banknotes Transfer
- Stateless: not based on the concept of “Account / Wallet Balance”, just focused on “Transaction Validity”
- Transaction is valid if

  `In_{t}.p <= Out_{t-1,id}.p`

  - the `In_{t}.p` = Facial Value of “Banknote” being spent now (at time t)
  - the `Out_{t-1,id}.p` = Facial Value of one of the “Banknotes” received at t-1
- Reminder (if any) gets sent back to the sender wallet / address

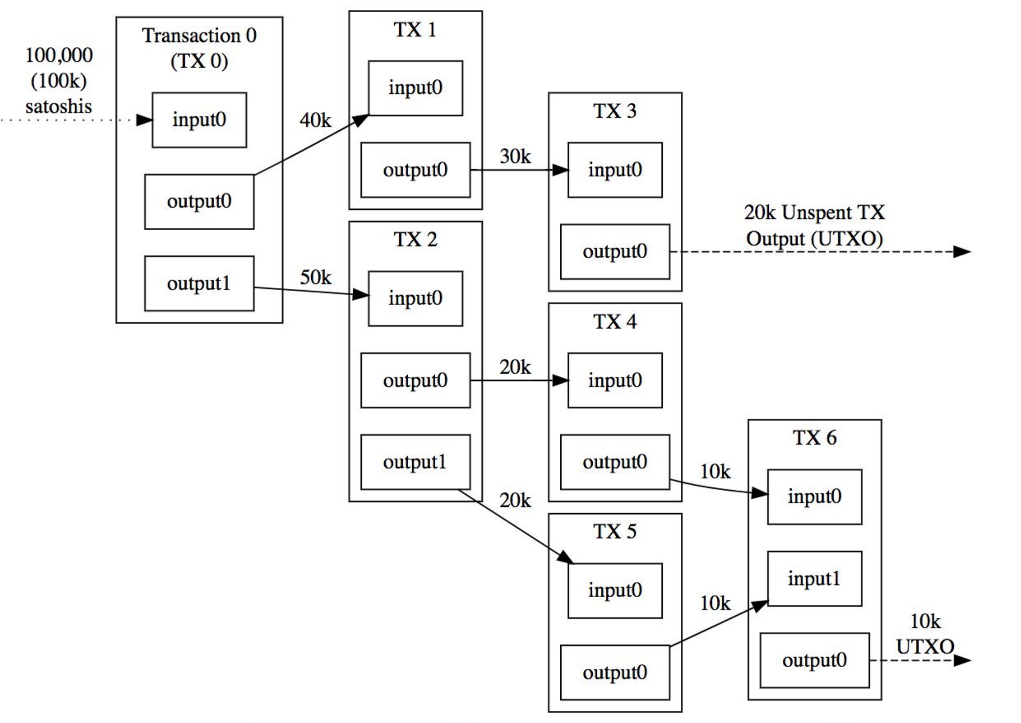
  `R = Out_{t-1,id}.p - In_{t}.p`

- If no owned Banknote is big enough, split in multiple Transactions

  `In_{t}.p > Out_{t-1,id}.p  \forall id`

  - then

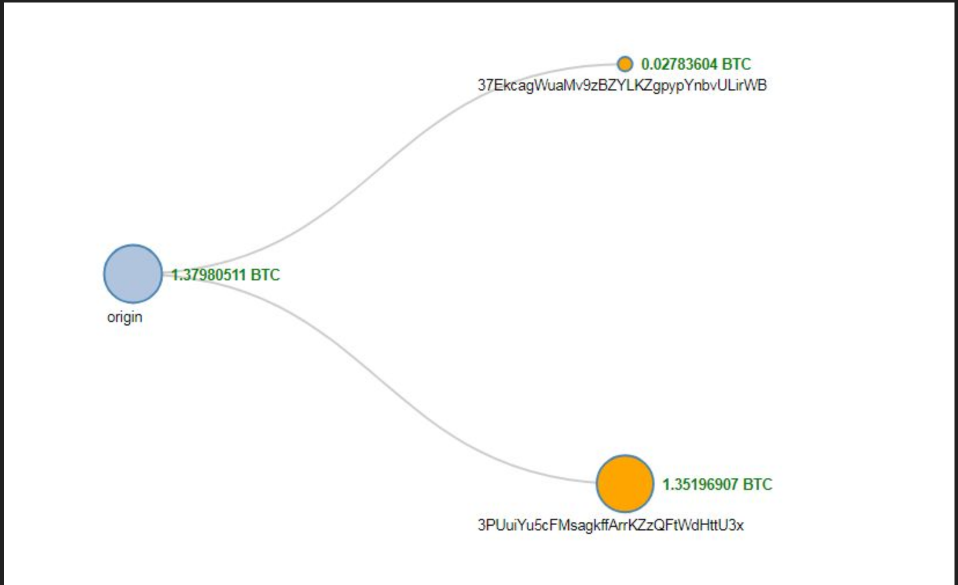
UTXO - Example



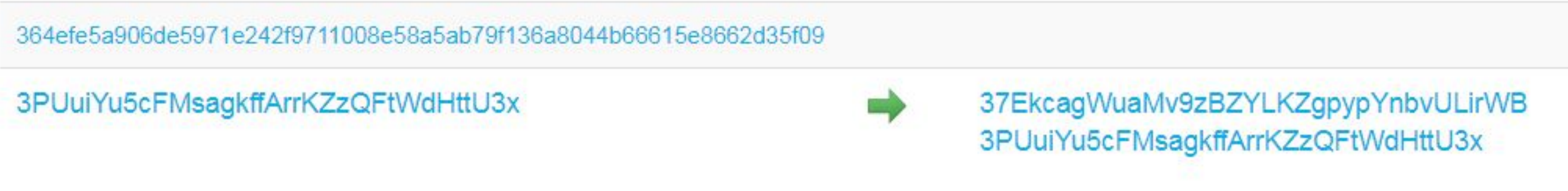
Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

- Inspired by Banknotes

UTXO - Reminder Example


0.02783604 BTC
37EkcagWuaMv9zBZYLKZgpypYnbvULirWB
1.37980511 BTC
origin
1.35196907 BTC
3PUuiYu5cFMsagkffArrKZzQFtWdHttU3x

- Source Addr: 3PU
- Dest Addr: 37E
- Observe the Transaction starting from 3PU sends In_{t}.p to 37E and Out_{t-1,id}.p - In_{t}.p back to 3PU
- See link


364efe5a906de5971e242f9711008e58a5ab79f136a8044b66615e8662d35f09

3PUuiYu5cFMsagkffArrKZzQFtWdHttU3x → 37EkcagWuaMv9zBZYLKZgpypYnbvULirWB
3PUuiYu5cFMsagkffArrKZzQFtWdHttU3x

Account Balance - Used in ETH

- Inspired by Bank Payments : no Banknotes, Account Balance tracked, Transactions = Account Balance updates
- Stateful: based on tracking each “Wallet Account Balance” explicitly
- Transfer is valid if

```
A.w.b >= Tx.p
```

  - The Sender Wallet Balance is >= Transaction Amount
- Compared to UTXO
  - Simpler
  - More Transparent : direct Wallet Balance tracking (no need to reconstruct it)