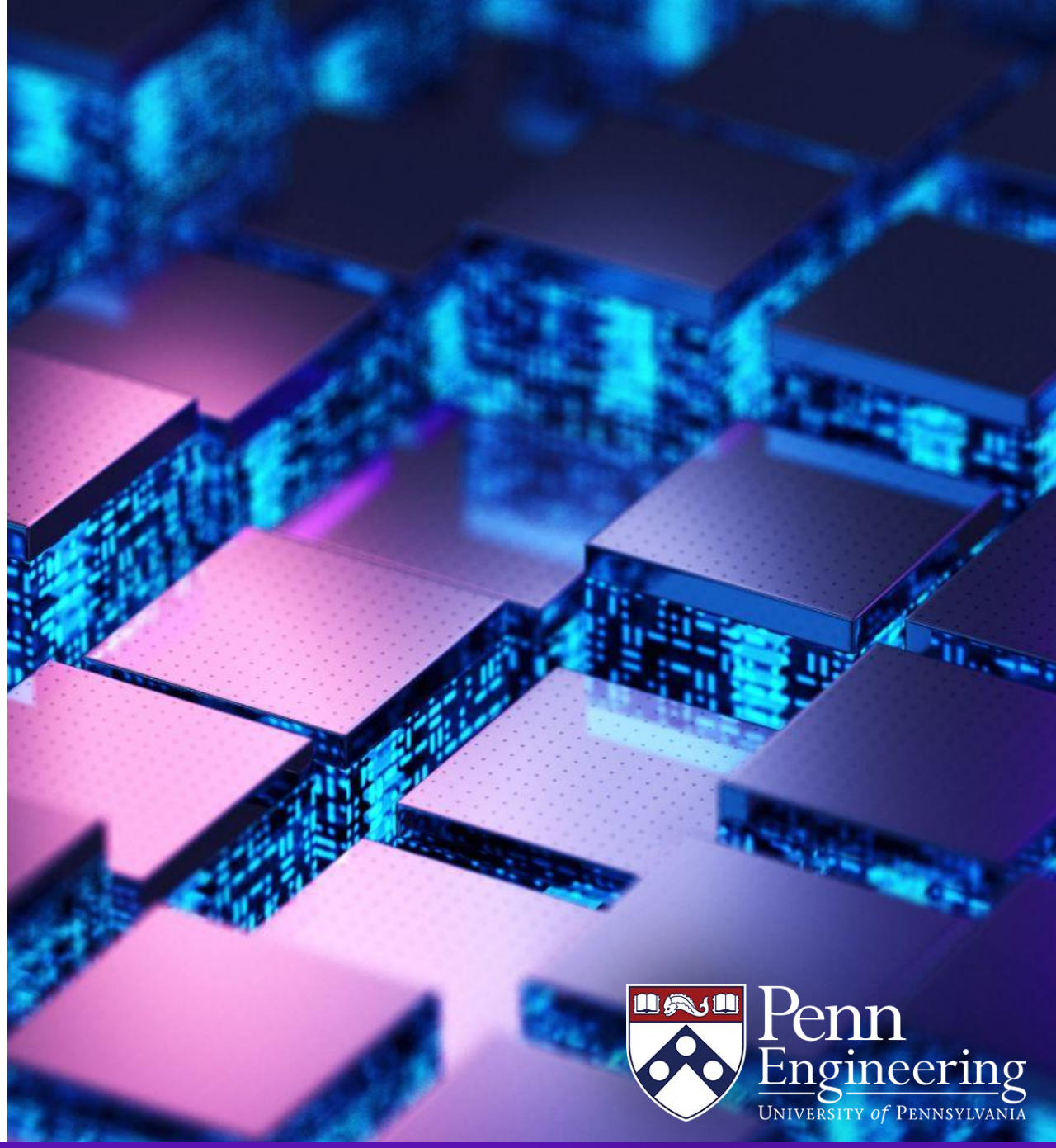
EAS 5830: BLOCKCHAINS

The UTXO Model

Professor Brett Hemenway Falk



Penn Engineering
University of Pennsylvania

How do you track balances on a ledger?

Account Balances

- EVM Chains
- Solana
- Algorand

UTXO

- Bitcoin
- ZCash
- Monero
- Cardano

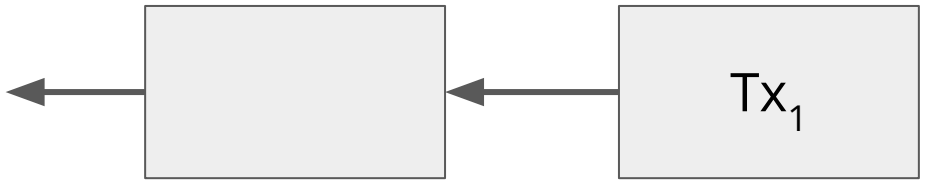
How do you track money on a ledger?

- Account-balances
  - EVM chains
  - Solana
  - Algorand
- UTXOs
  - Bitcoin
  - ZCash
  - Monero
  - Cardano

The UTXO Model

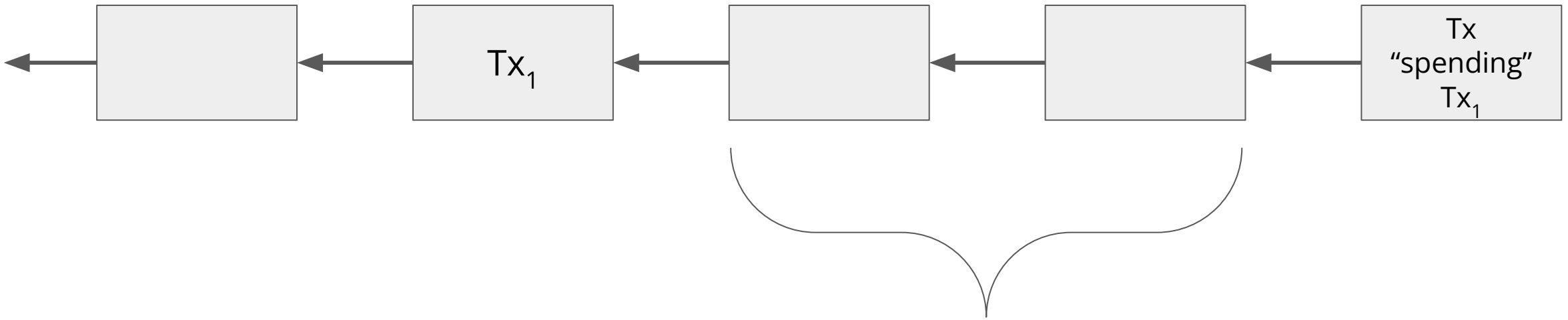
- Every transaction has inputs and outputs
  - Every output is associated with an address (or a simple script)
- Each output can be “spent” once, i.e., each output can only be used as the input to a single transaction
- Outputs cannot be partially spent (transactions must make “change”)
- Unspent Transaction Outputs are called UTXOs

Verifying Transactions (UTXO Model)



Verifying Transactions (UTXO Model)

Verifying Transactions (UTXO Model)



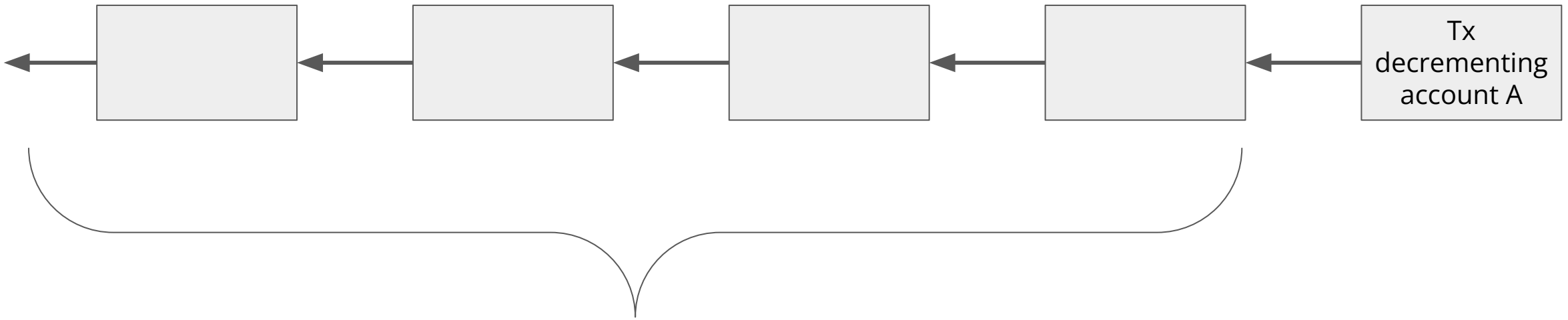
Check all subsequent transactions to make sure Tx_1 was not spent

Verifying Transactions (UTXO Model)

Everything your node does to verify the historical blockchain is done with the sole purpose of building the UTXO set.

Verifying Transactions (Account Balance Model)

Verifying Transactions (Account Balance Model)



Check all previous transactions to ensure A has sufficient balance

Including state in account-balance model

- To eliminate the need to repeatedly parse the chain, ledgers in the account-balance model include *complete state* (all account balances) in each block
- State is compressed
  - In Ethereum world state is stored in Merkle-Patricia Tree
  - Each block includes only updated nodes in the tree

Comparison

- UTXO model
  - Better privacy?
    - Each user is encourage to have a separate address for each UTXO
    - Multi-input transactions obscure the analysis
    - Still easy to follow “tainted” UTXO (in the event of money-laundering or theft)
  - Better parallelism?

- Account model
  - Each user is encouraged to have 1 address
    - Otherwise system must track many 0-balance addresses
      - Algorand has minimum balance
      - Solana charges “rent”
  - Money is fungible
  - Easier to support smart contracts

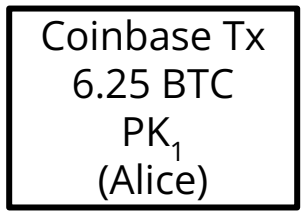
Replay Attacks

- Digital signatures verify source of message (transaction)
- Signed messages can be copied
  - Account model
    - Send 5 ETH from account A to account B (signed by A)
    - **How can validator distinguish recurring payment from replay attack?**
  - UTXO model
    - Send 5 BTC from UTXO H to account B
    - **Validators check that each Tx input has never been spent before**

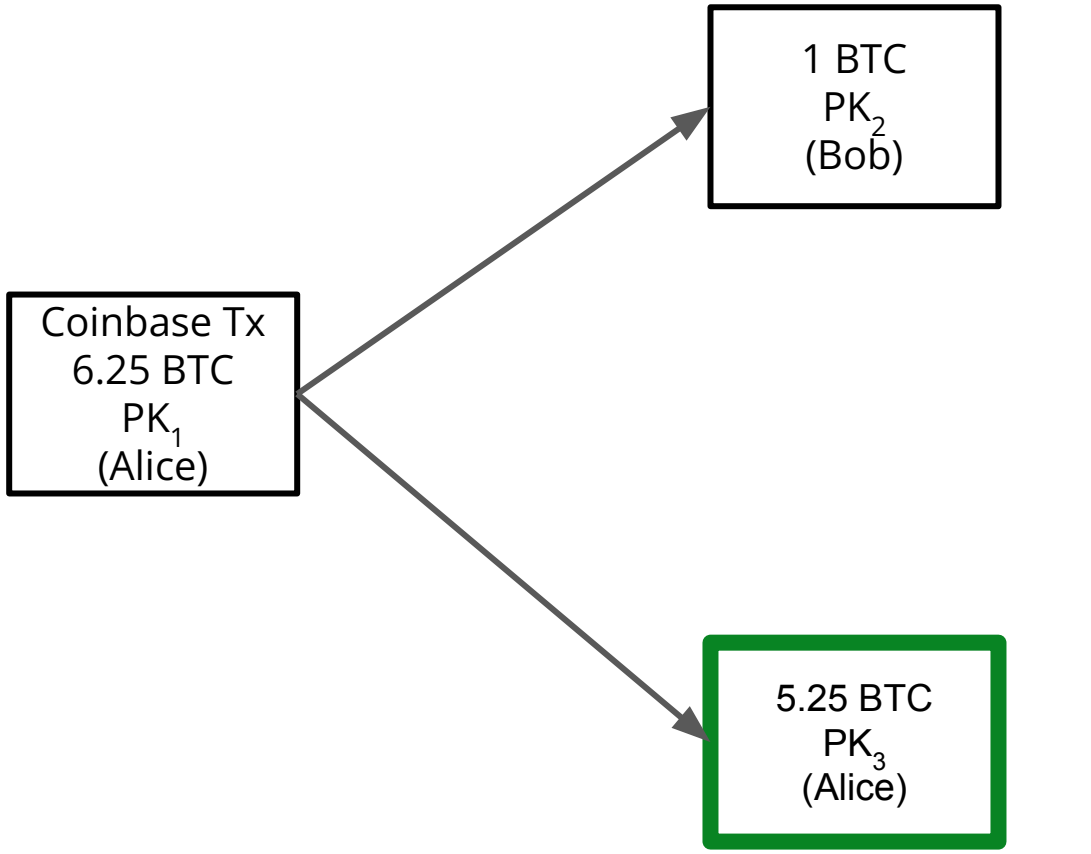
Transaction Nonces

- To prevent replay attacks in the account model, each account maintains a counter (called a “nonce”), counting the number of transactions *sent* from this account.
- Transaction is only valid if counter is larger than all previous counters used by this address
- No transaction nonces necessary in UTXO model

Making change

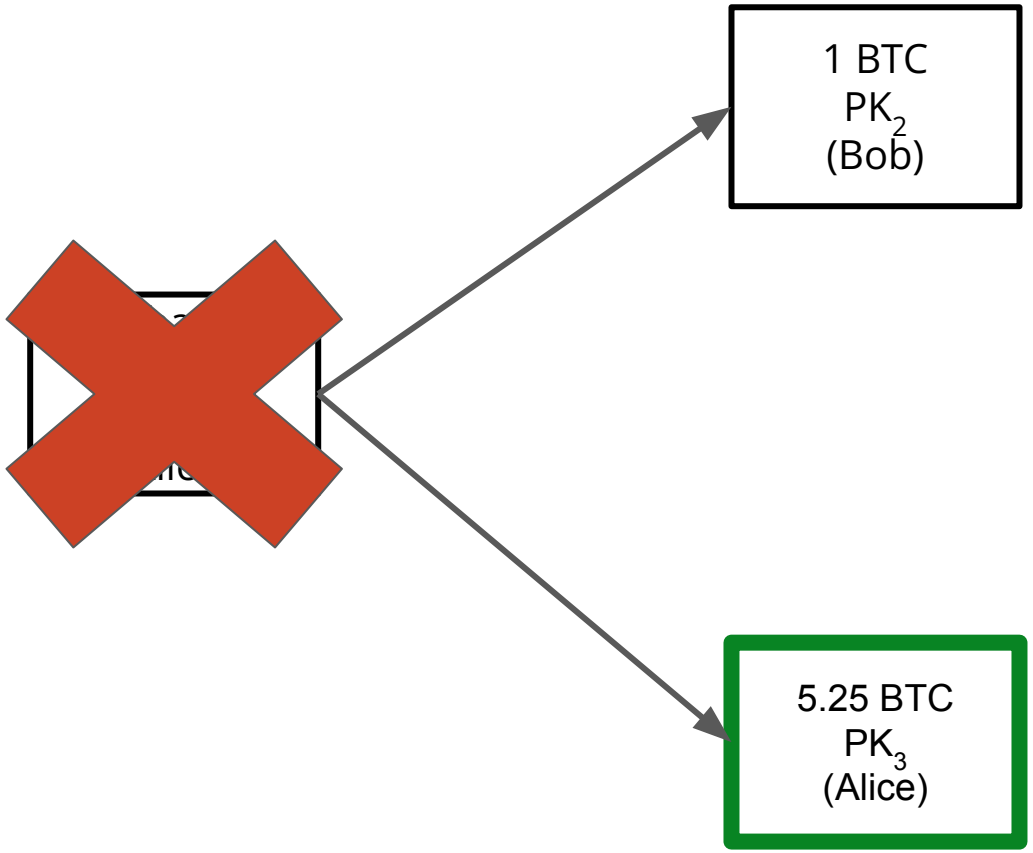


Making change



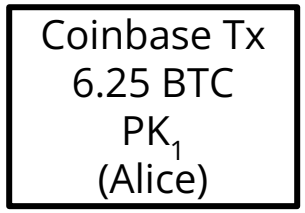
Outputs must sum up to input

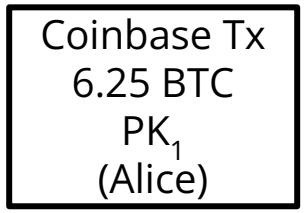
Making change



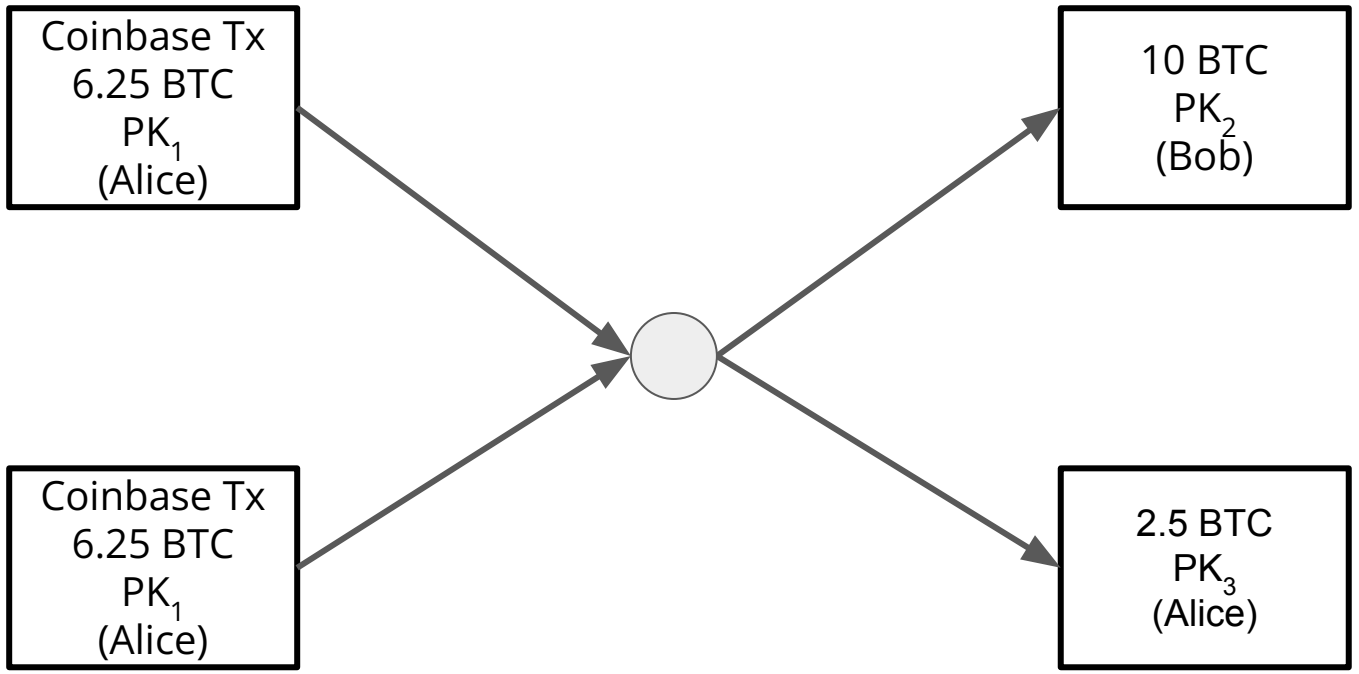
Outputs must sum up to input

Multiple inputs

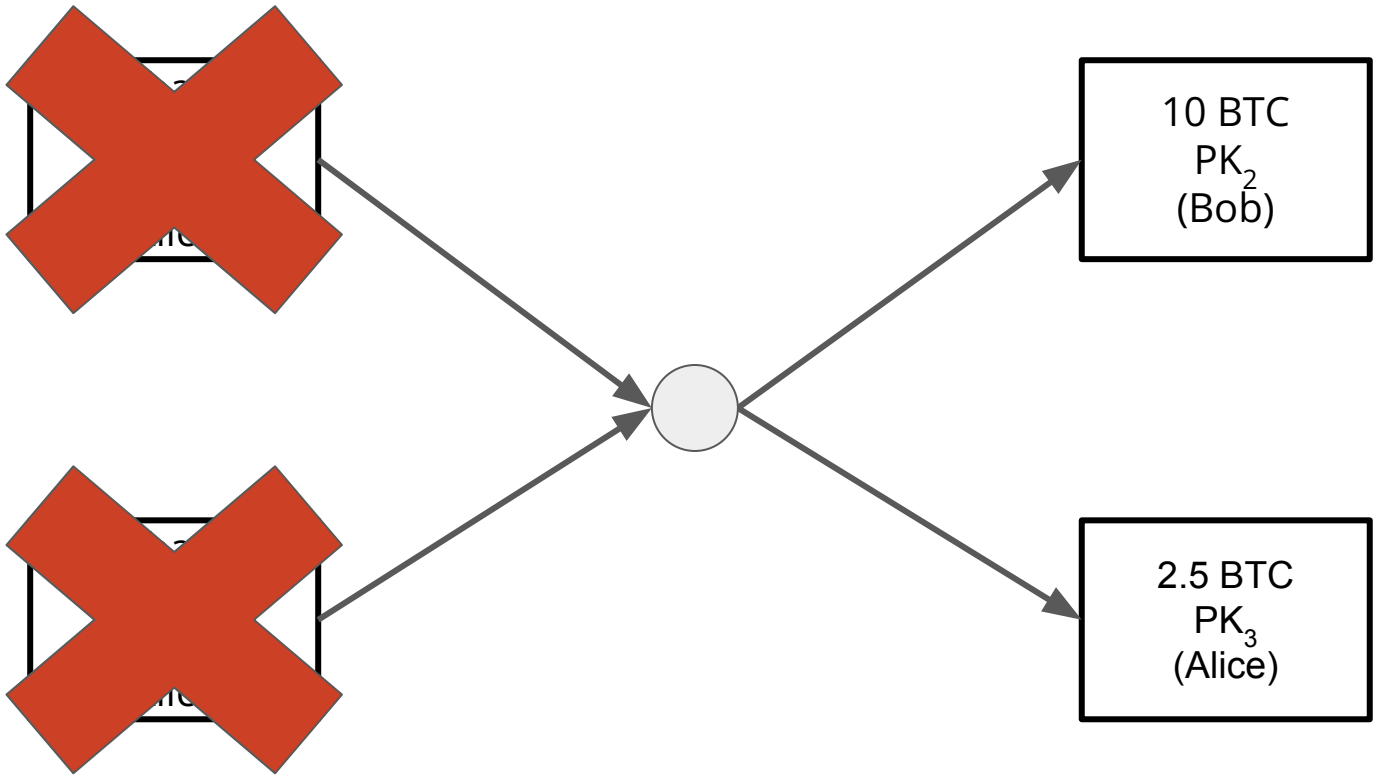




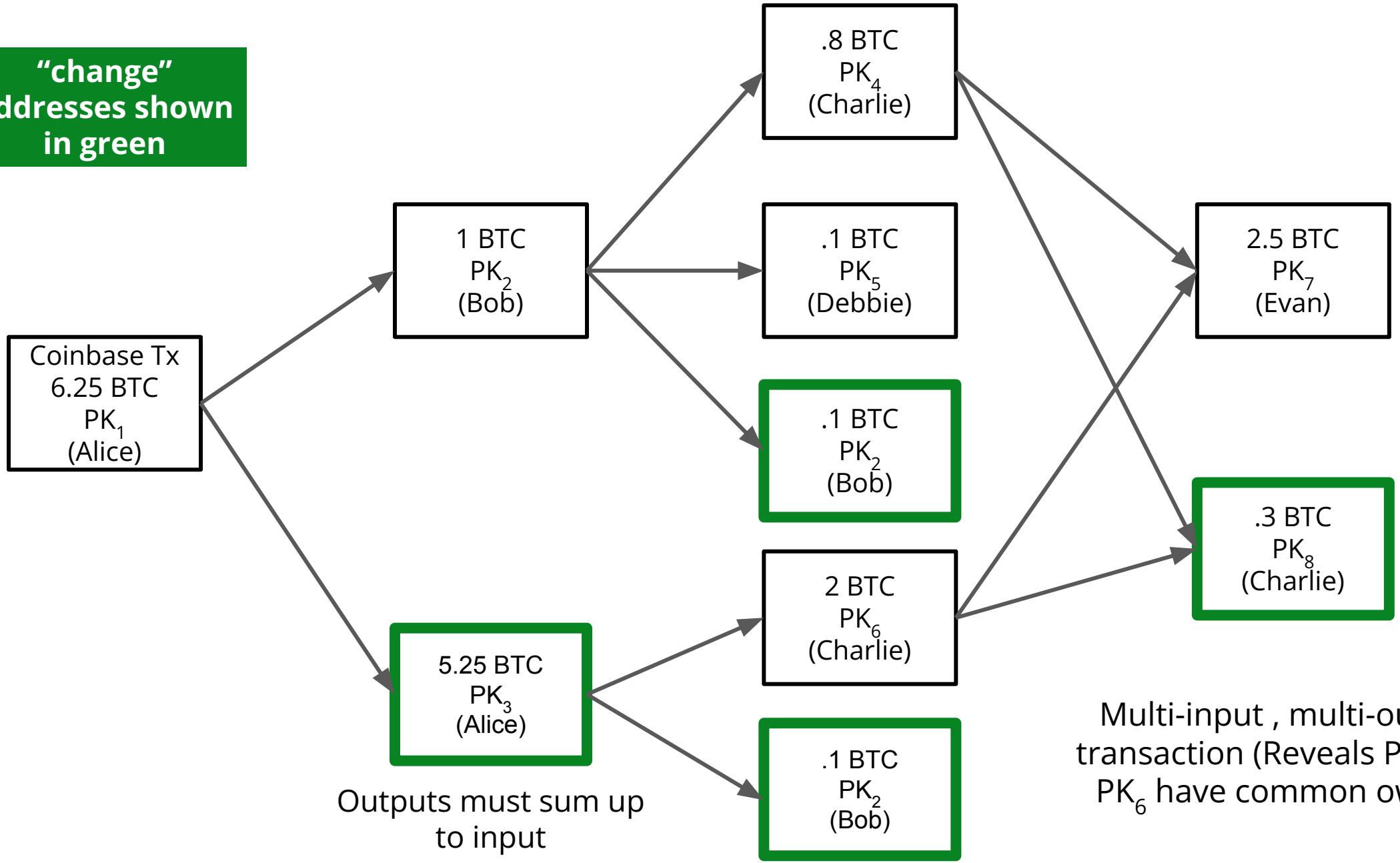
Multiple inputs



Multiple inputs



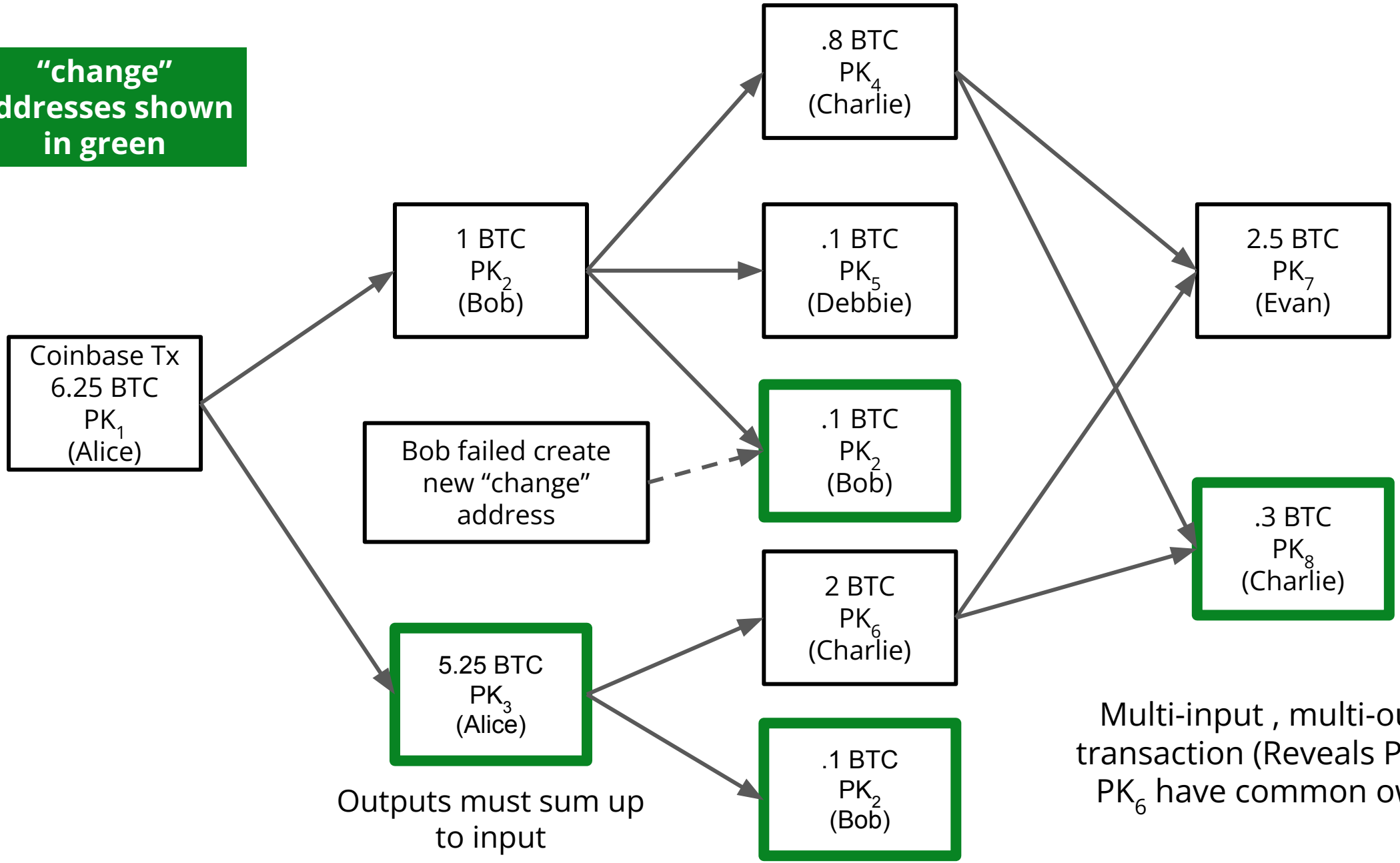
"change" addresses shown in green



Outputs must sum up to input

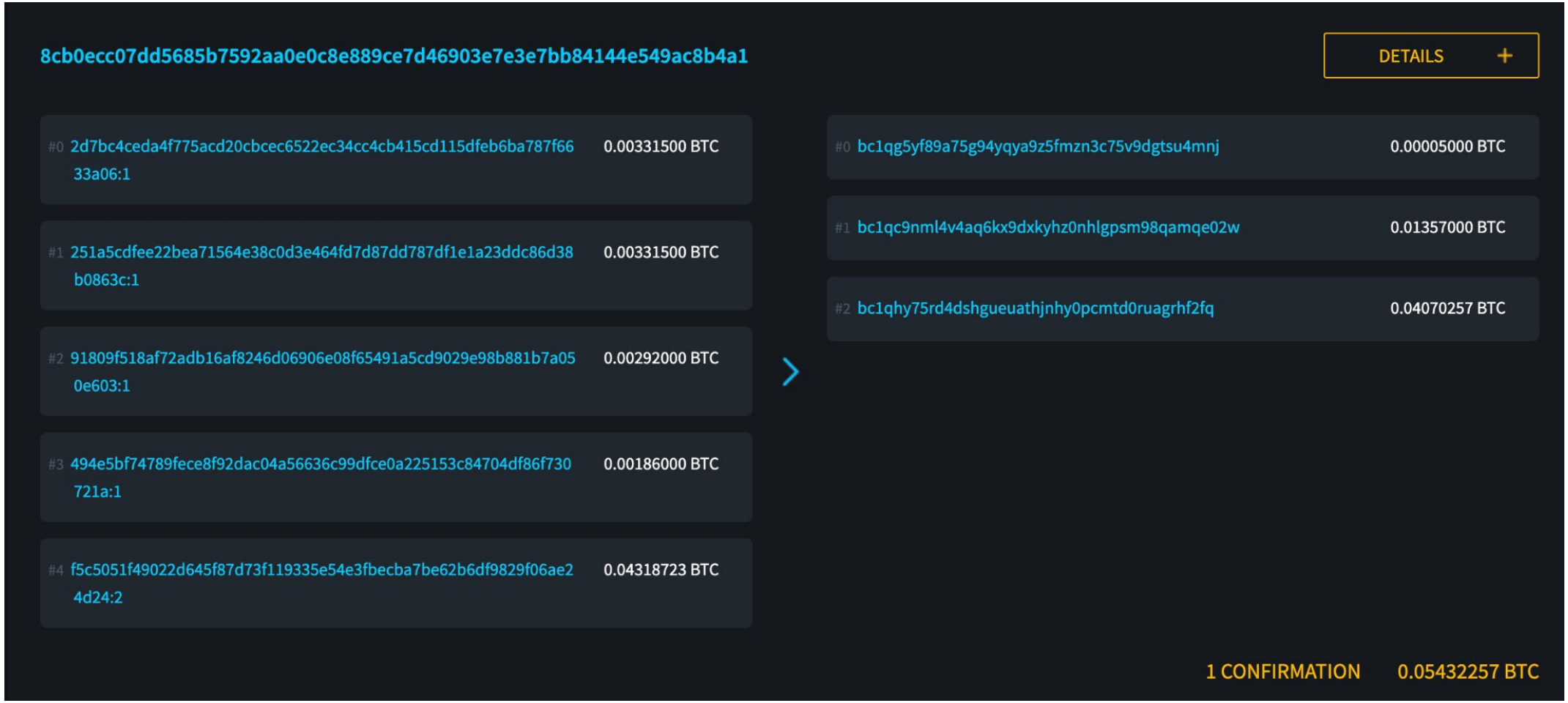
Multi-input , multi-output transaction (Reveals PK_4 and PK_6 have common owner)

"change" addresses shown in green



Outputs must sum up to input

Multi-input , multi-output transaction (Reveals PK_4 and PK_6 have common owner)


8cb0ecc07dd5685b7592aa0e0c8e889ce7d46903e7e3e7bb84144e549ac8b4a1
DETAILS
#0 2d7bc4ceda4f775acd20cbcec6522ec34cc4cb415cd115dfeb6ba787f6633a06:1 0.00331500 BTC
#1 251a5cdfee22bea71564e38c0d3e464fd7d87dd787df1e1a23ddc86d38b0863c:1 0.00331500 BTC
#2 91809f518af72adb16af8246d06906e08f65491a5cd9029e98b881b7a050e603:1 0.00292000 BTC
#3 494e5bf74789fece8f92dac04a56636c99dfce0a225153c84704df86f730721a:1 0.00186000 BTC
#4 f5c5051f49022d645f87d73f119335e54e3fbecba7be62b6df9829f06ae24d24:2 0.04318723 BTC
#0 bc1qg5yf89a75g94yqya9z5fmzn3c75v9dgtsu4mnj 0.00005000 BTC
#1 bc1qc9nml4v4aq6kx9dxkyhz0nhlgpsm98qamqe02w 0.01357000 BTC
#2 bc1qhy75rd4dshgueuathjnhy0pcmtd0ruagrhf2fq 0.04070257 BTC
1 CONFIRMATION
0.05432257 BTC

Industry Execs Claim Freshly Minted 'Virgin Bitcoins' Fetch 20% Premium

The Virgin Bitcoin Fallacy

Miners have begun to promote "clean bitcoin" with guarantees on climate, KYC and and OFAC compliance. But are such coins even possible?

By Nic Carter May 11, 2021 at 11:27 a.m. EDT

What Are Ordinals? A Beginner's Guide to Bitcoin NFTs

The Bitcoin community has gone wild over Ordinal Inscriptions, but what is the new thing taking over Crypto Twitter?

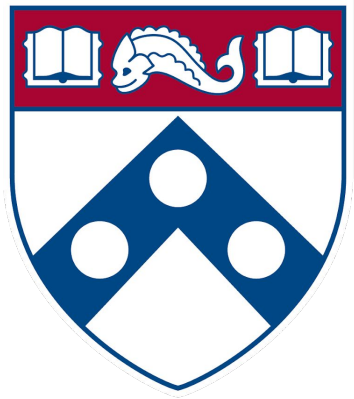
By Jason Nelson

Nov 8, 2023

4 min read

Ordinals

- Number every sat in the order in which it is mined.
  - These numbers are termed "ordinal numbers", or "ordinals", as they are ordinal numbers in the mathematical sense
- The ordinal numbers of sats in transaction inputs are transferred to output sats in first-in-first-out order, according to the size and order of the transactions inputs and outputs.



Penn
Engineering
UNIVERSITY of PENNSYLVANIA