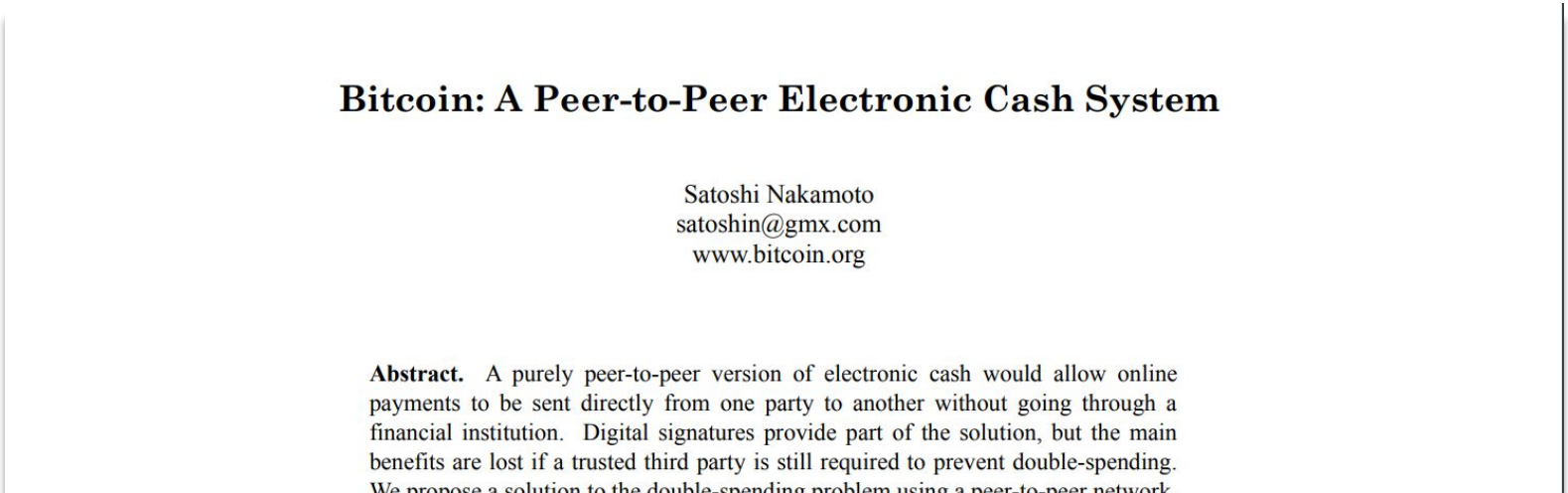
Image source: 'New Super Mario Bros. 2' players have collected over 10 billion coins

Pramod is not giving financial advice :)

Who is *Satoshi Nakamoto*?

- Aug. 18, 2008: bitcoin.org is registered
- Oct. 31, 2008: white paper posted to cryptography mailing list
- Satoshi Nakamoto is unknown to this day!



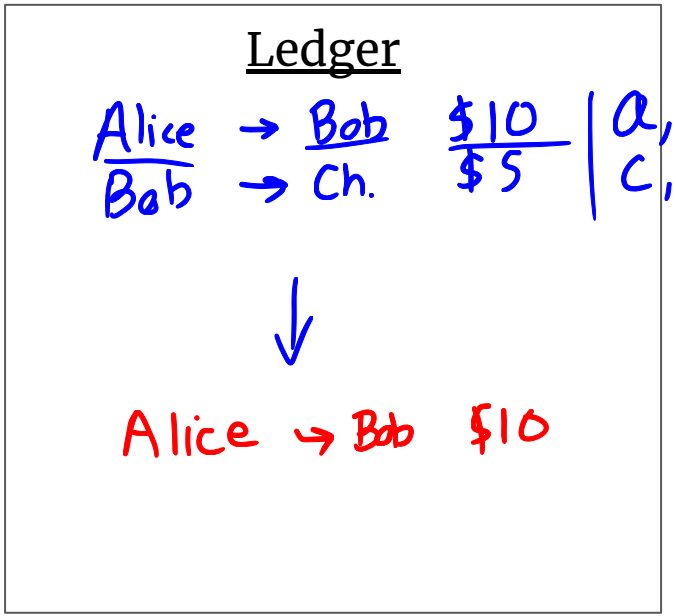
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network

What's in a ledger?

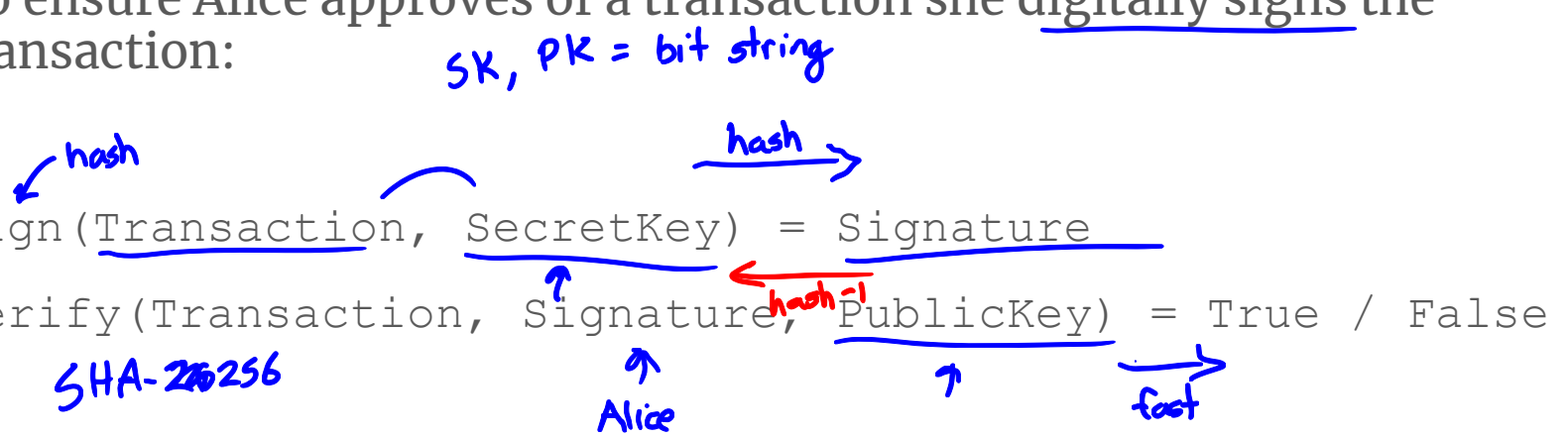
- Alice, Bob, and Charlie are friends: exchange money & settle on the 1st
- A ledger is a list of transactions:



Transaction:
- Sender
- Recipient
- Amount

Preventing fake transactions

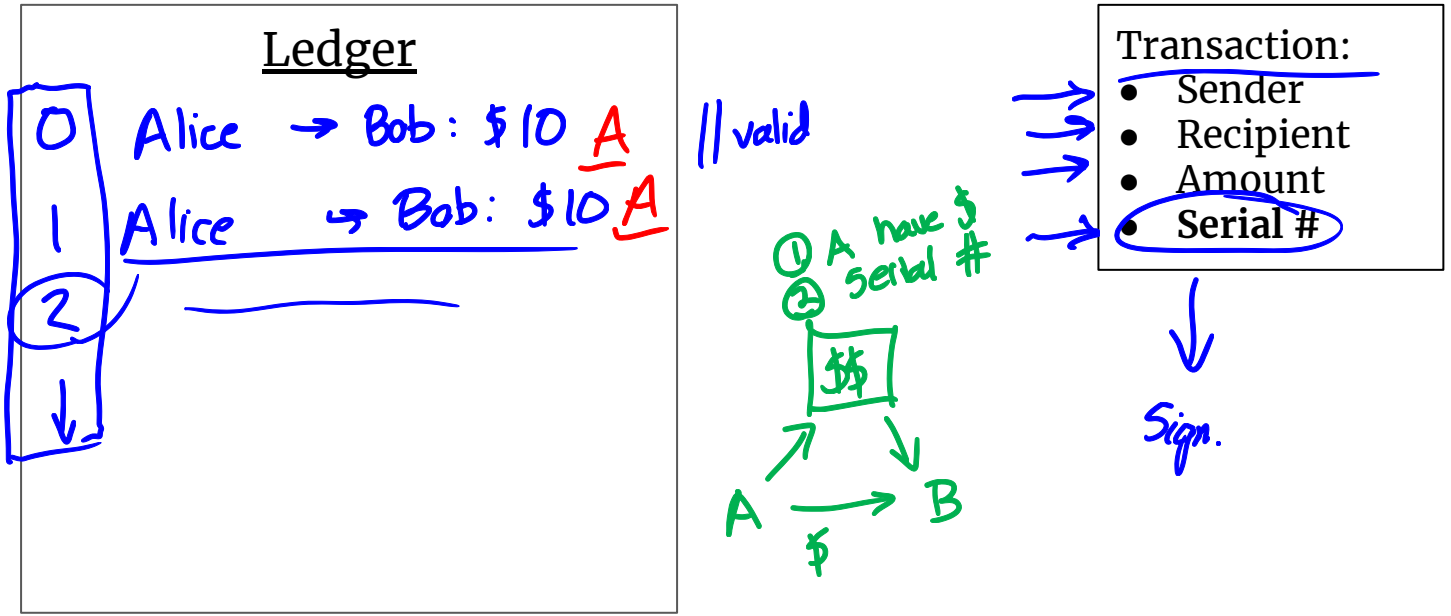
To ensure Alice approves of a transaction she digitally signs the transaction:



Sign takes the form of a cryptographic hash function like SHA-256. Any manipulation of the `Transaction` causes the `Signature` to change *seemingly randomly*. **It's infeasible to fake the `Signature`.**

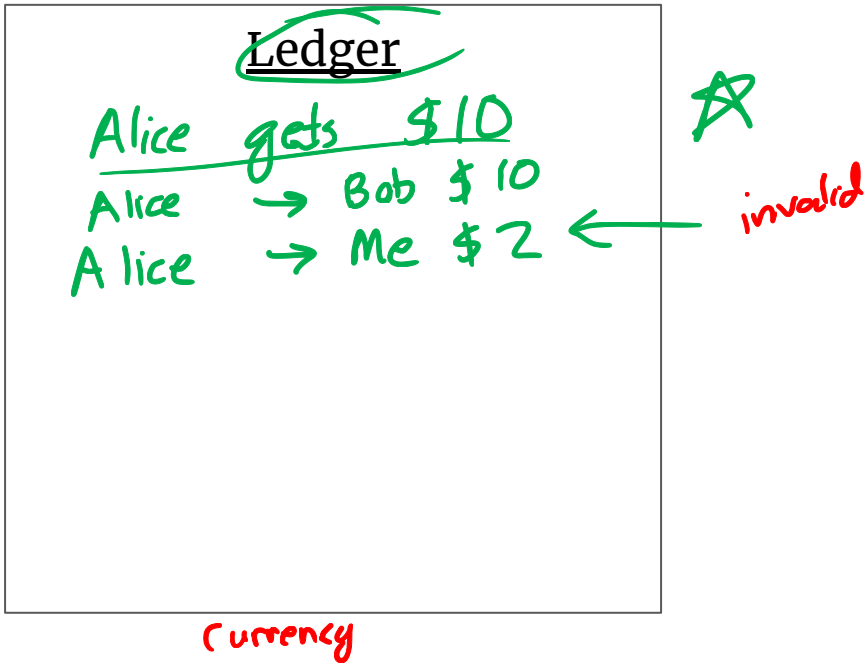
Preventing duplicate transactions

- Alice can send money to Bob multiple times -> use a serial number



Preventing overspending

What if Alice tries to overspend?



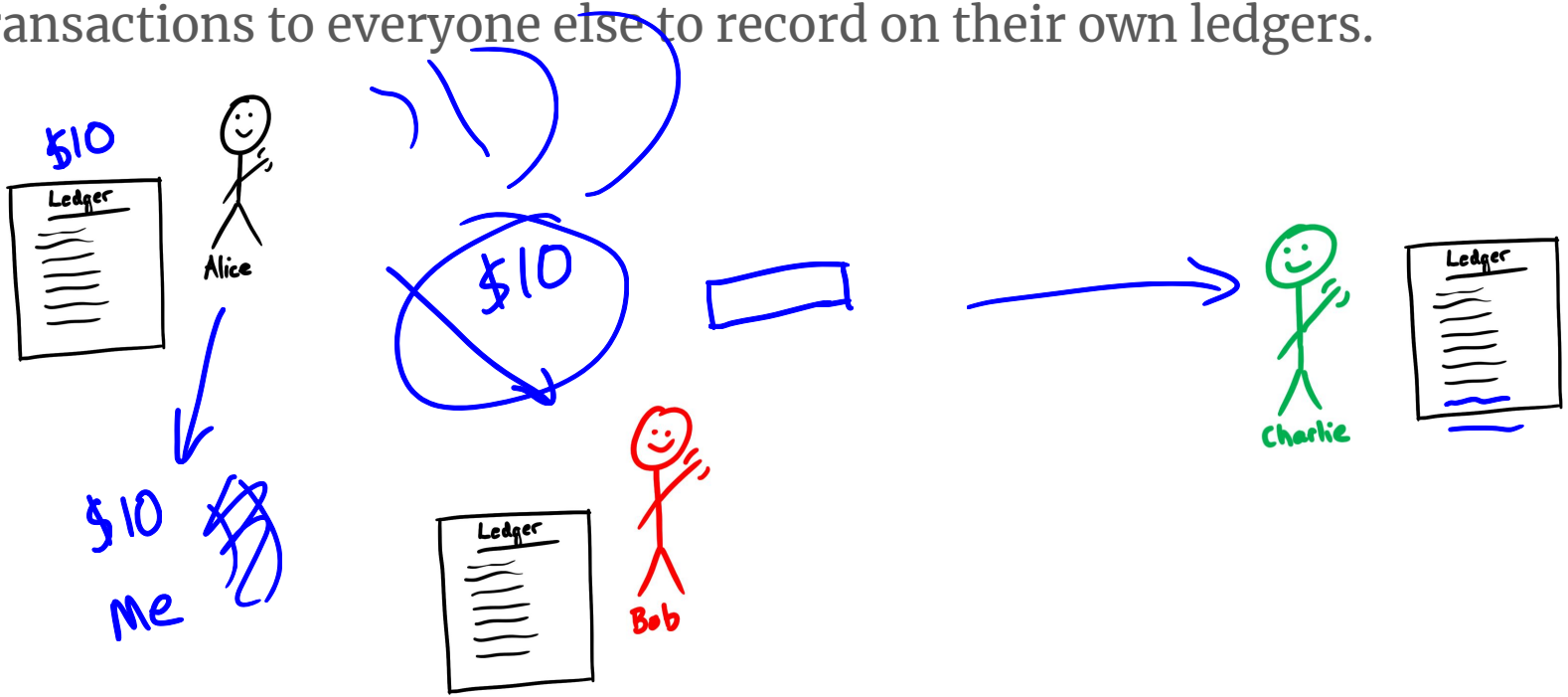
Transaction:
- Sender
- Recipient
- Amount
- **Serial #**

Alice's running balance:

~~$10~~
~~$0~~

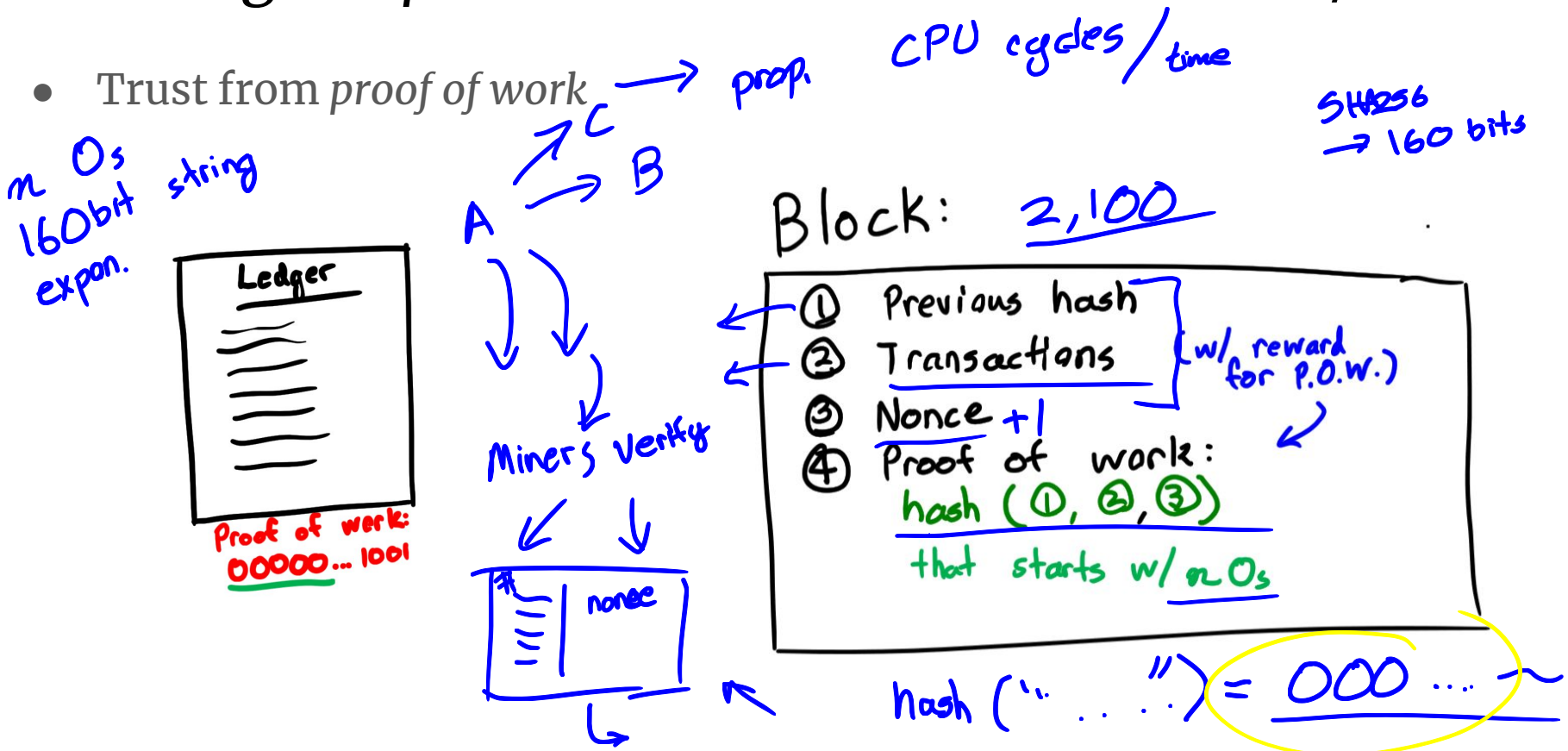
Trusted third party -> decentralized trust model

Everyone keeps their own copy of the ledger, broadcasting new transactions to everyone else to record on their own ledgers.

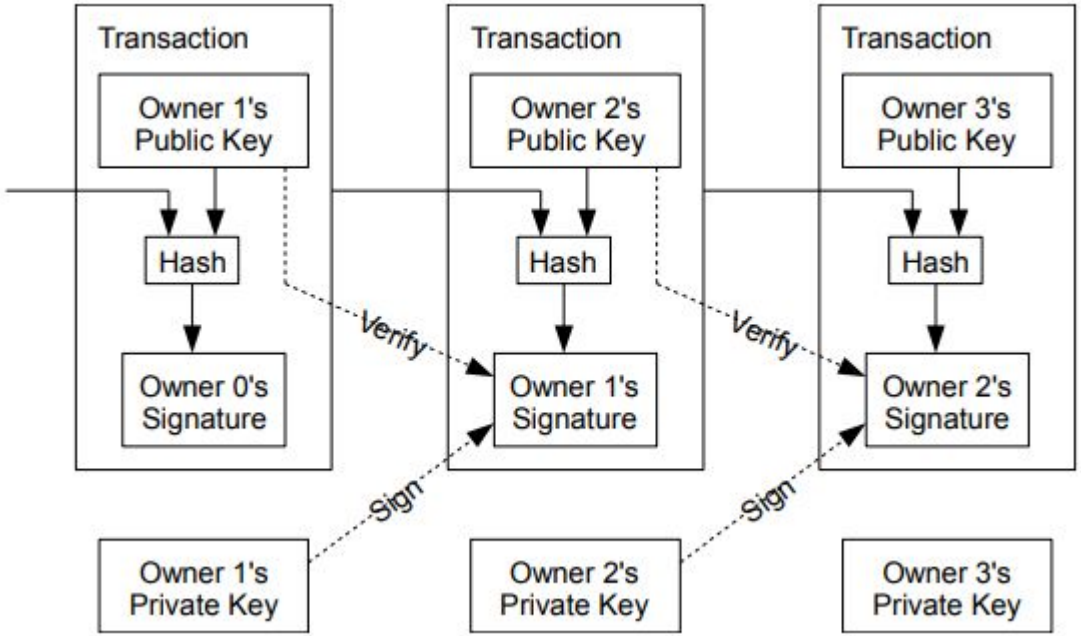


Trusting *computational work* instead of a mint/bank

- Trust from *proof of work*

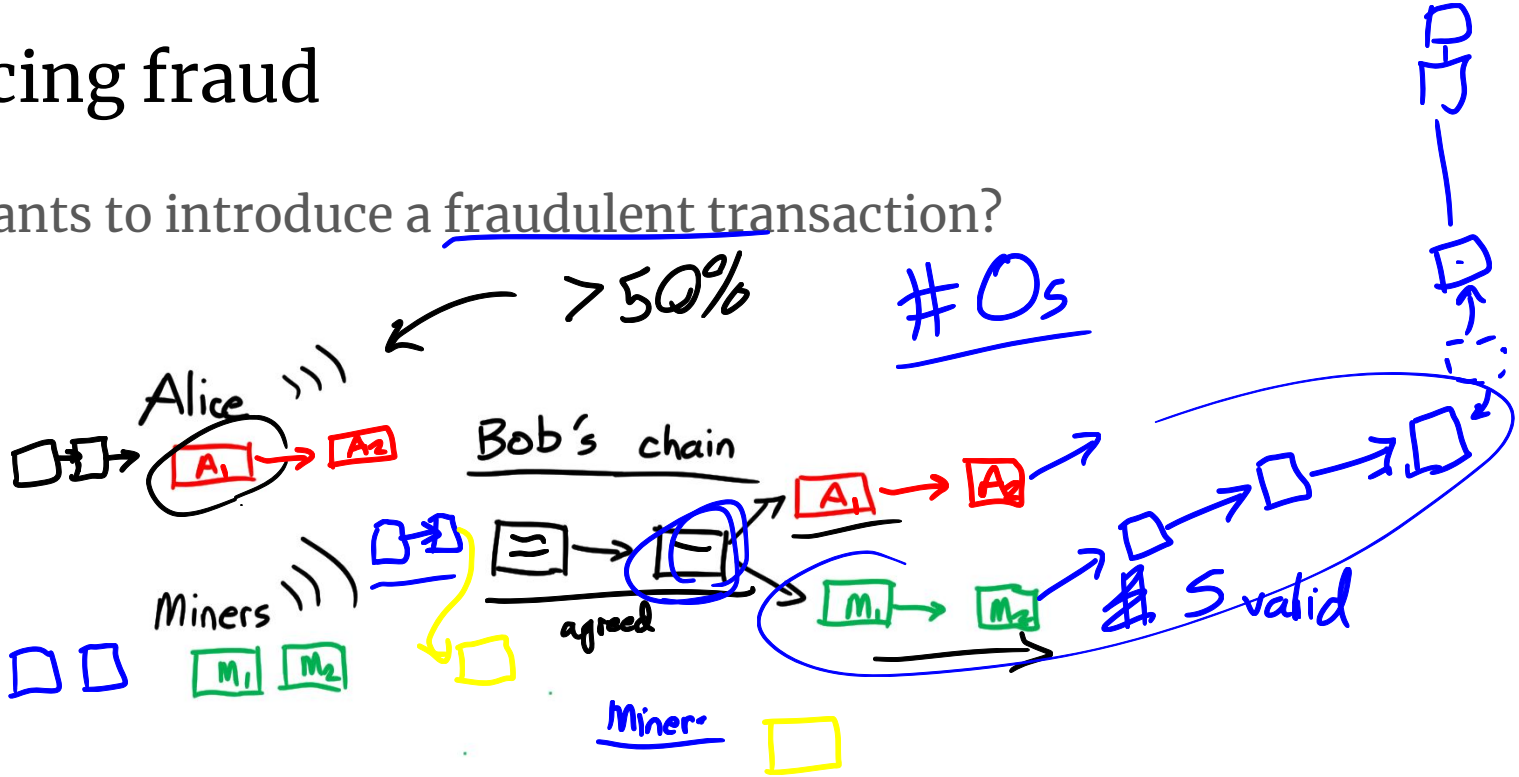


Welcome to the blockchain!



Introducing fraud

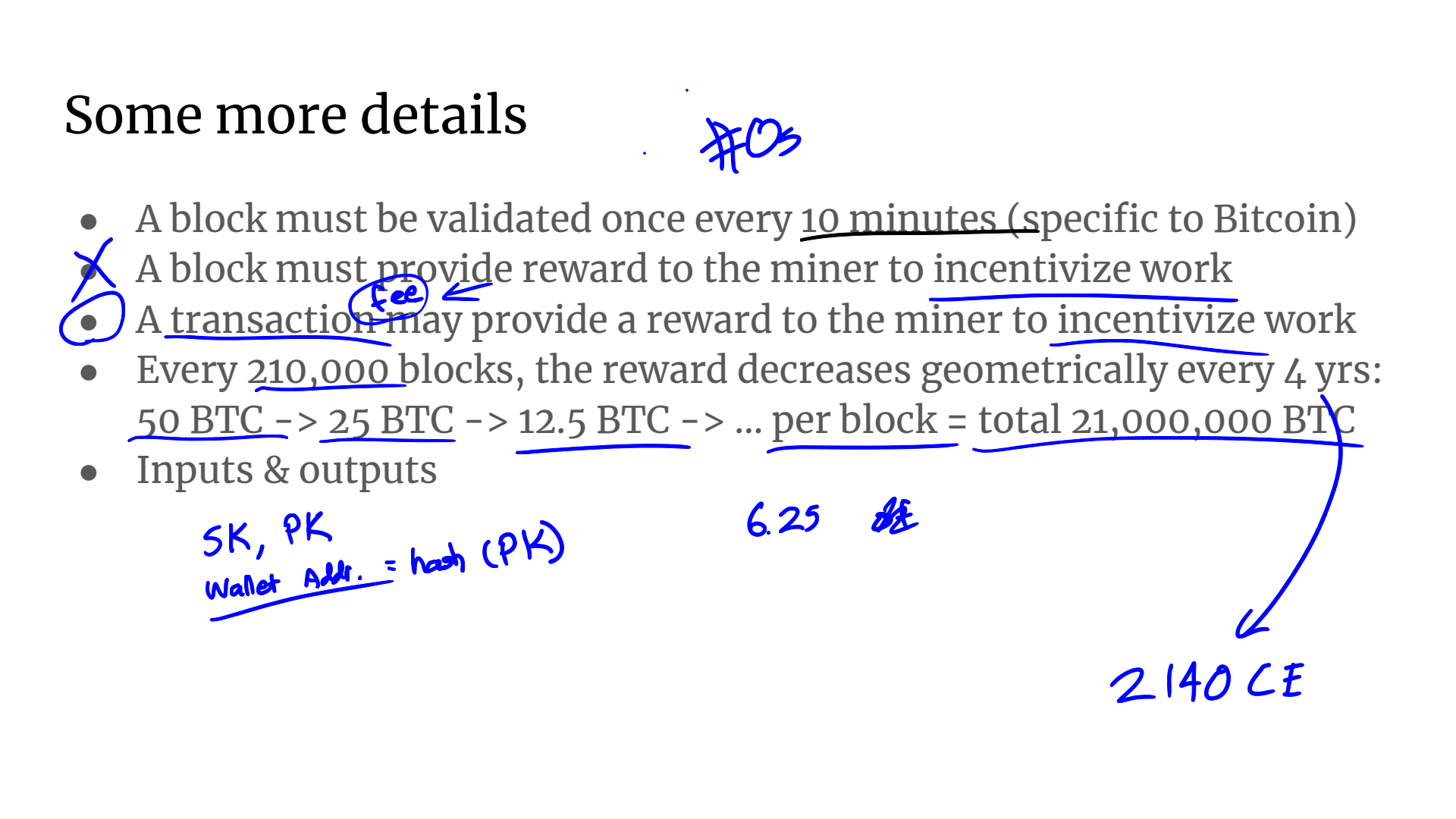
Say Alice wants to introduce a fraudulent transaction?



By following the *longest chain* (i.e. the one with the most *work*), we rely on the network to tell us if a block (and it's transactions are valid)

Some more details

- A block must be validated once every 10 minutes (specific to Bitcoin)
- A block must provide reward to the miner to incentivize work
- A transaction may provide a reward to the miner to incentivize work
- Every 210,000 blocks, the reward decreases geometrically every 4 yrs: 50 BTC -> 25 BTC -> 12.5 BTC -> ... per block = total 21,000,000 BTC
- Inputs & outputs



```
{"hash":"993830...",
"ver":1,
"vin_sz":3,
 "vout_sz":2,
 "lock_time":0,
 "size":552,
 "in":[
   {"prev_out":{
     "hash":"3beabc...",
        "n":0},
    "scriptSig":"304402... 04c7d2..."},
   {"prev_out":{
        "hash":"fdae9b...",
        "n":0},
     "scriptSig":"304502... 026e15..."},
   {"prev_out":{
        "hash":"20c86b...",
        "n":1},
     "scriptSig":"304402... 038a52..."}],
 "out":[
   {"value":"0.01068000",
     "scriptPubKey":"OP_DUP OP_HASH160 e8c306... OP_EQUALVERIFY OP_CHECKSIG"},
   {"value":"4.00000000",
     "scriptPubKey":"OP_DUP OP_HASH160 d644e3... OP_EQUALVERIFY OP_CHECKSIG"}]}
```

Core assumptions

1. Cryptographic hashes are computationally infeasible to reverse

2. Transactions (through blocks) must provide *proof of work* as trust

3. The majority of nodes on a blockchain network are “honest brokers”

CPU power

Image source: 'New Super Mario Bros. 2' players have collected over 10 billion coins

Pramod is not giving financial advice :)

References

A Peer-to-Peer Electronic Cash System

How the Bitcoin protocol actually works | DDI

Bitcoin Wiki

But how does bitcoin actually work?