LECTURE 1

BLOCKCHAIN BASICS

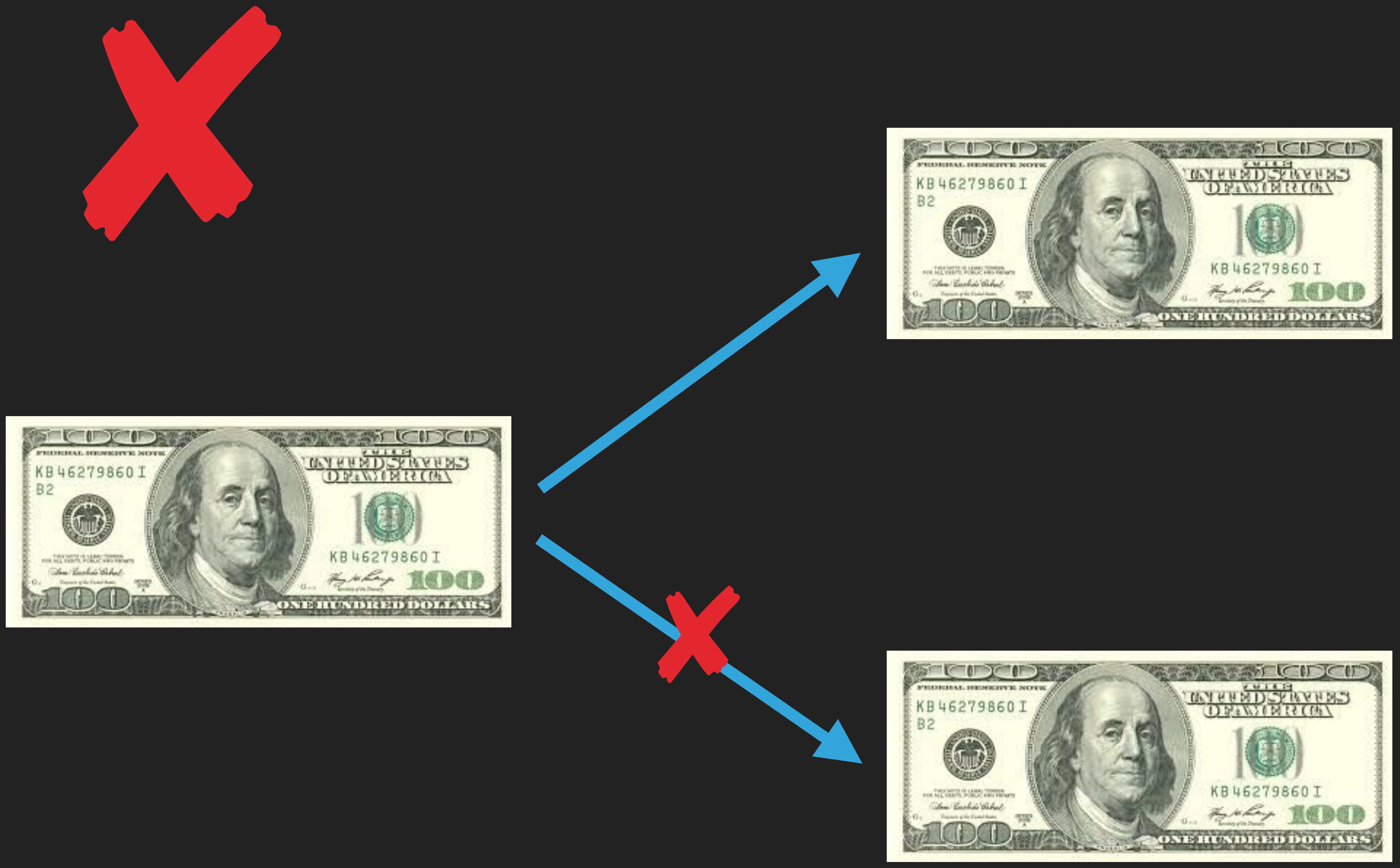
BITCOIN:
A PEER-TO-PEER ELECTRONIC CASH SYSTEM

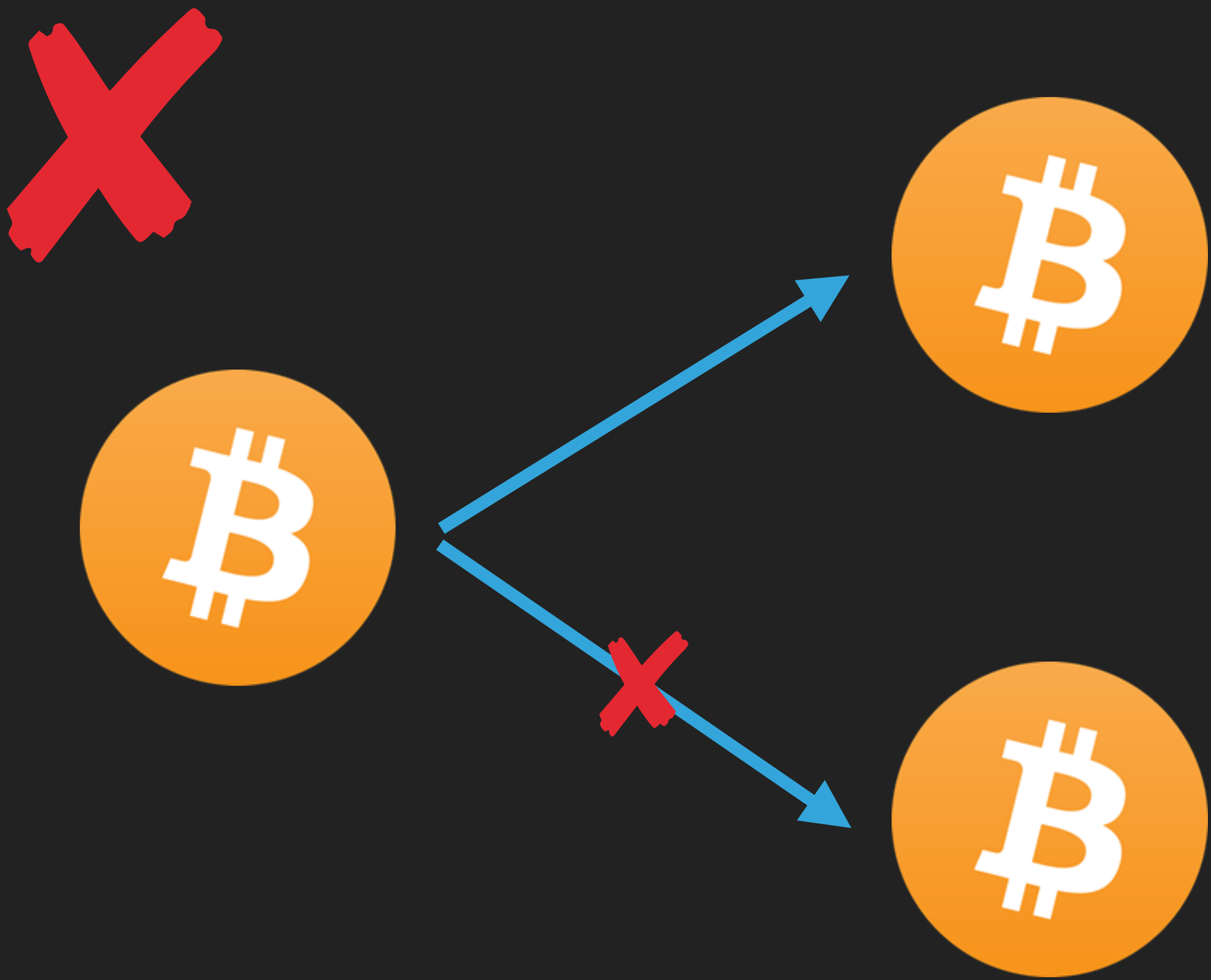
— SATOSHI NAKAMOTO

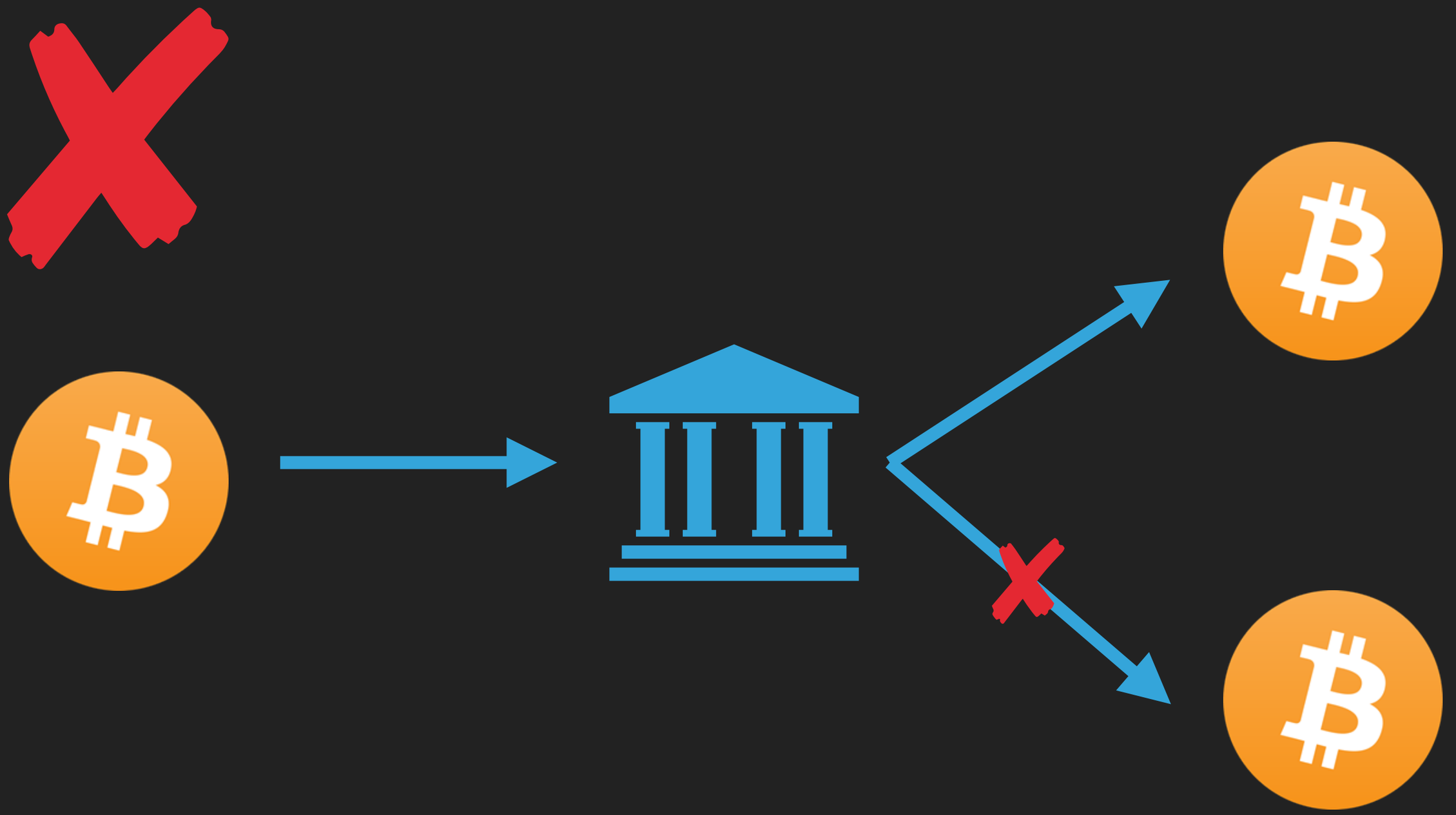
THE FUNDAMENTAL PROBLEM:

DOUBLE SPENDING

IN A DECENTRALIZED ENVIRONMENT


FEDERAL RESERVE NOTE
KB46279860I
B2
THE UNITED STATES OF AMERICA
KB46279860I
100
ONE HUNDRED DOLLARS
FEDERAL RESERVE NOTE
KB46279860I
B2
THE UNITED STATES OF AMERICA
KB46279860I
100
ONE HUNDRED DOLLARS
FEDERAL RESERVE NOTE
KB46279860I
B2
THE UNITED STATES OF AMERICA
KB46279860I
100
ONE HUNDRED DOLLARS





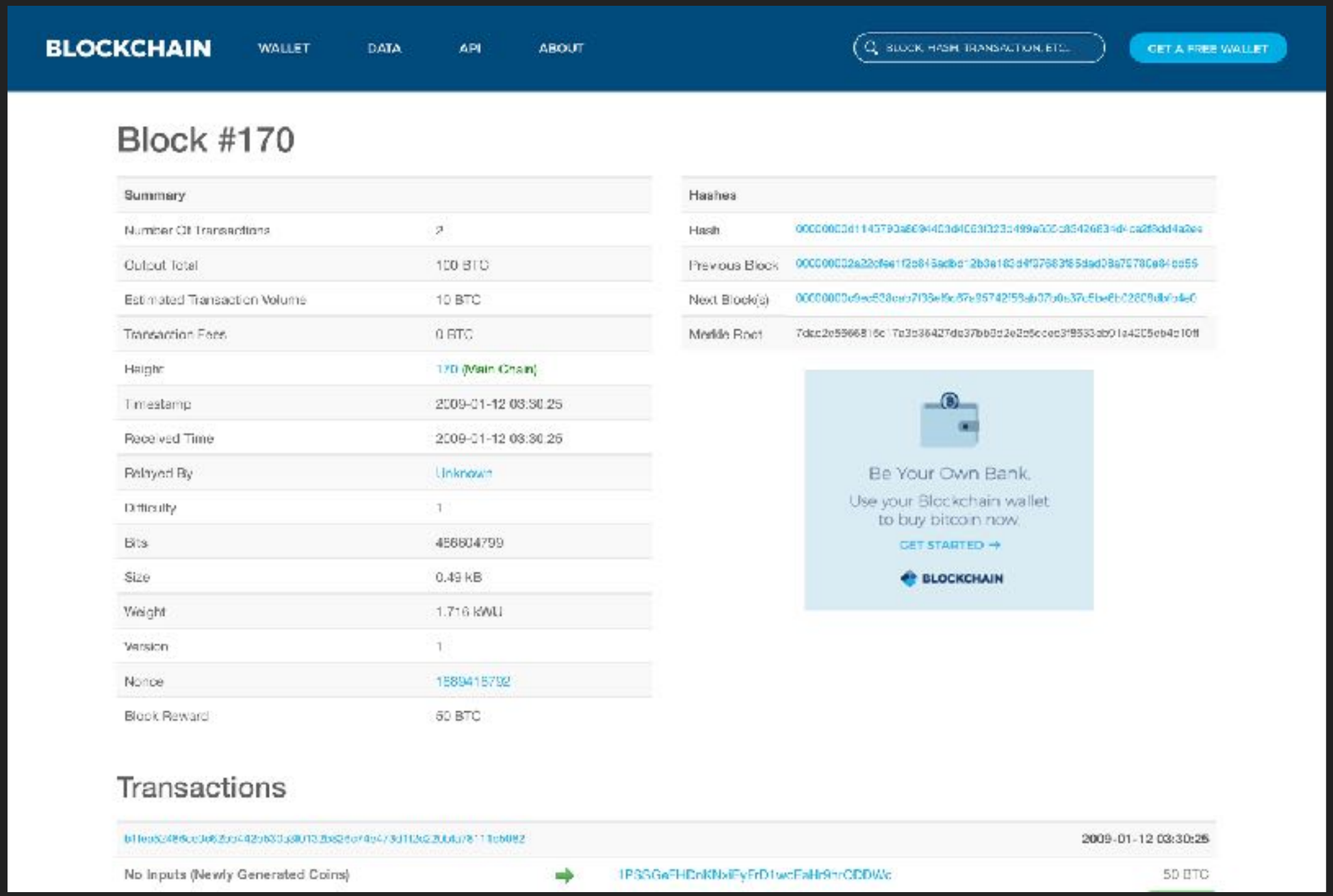

FEDERAL RESERVE NOTE
KB46279860I
B2
THE UNITED STATES OF AMERICA
100
KB46279860I
100
ONE HUNDRED DOLLARS

BOTH ARE P2P =)

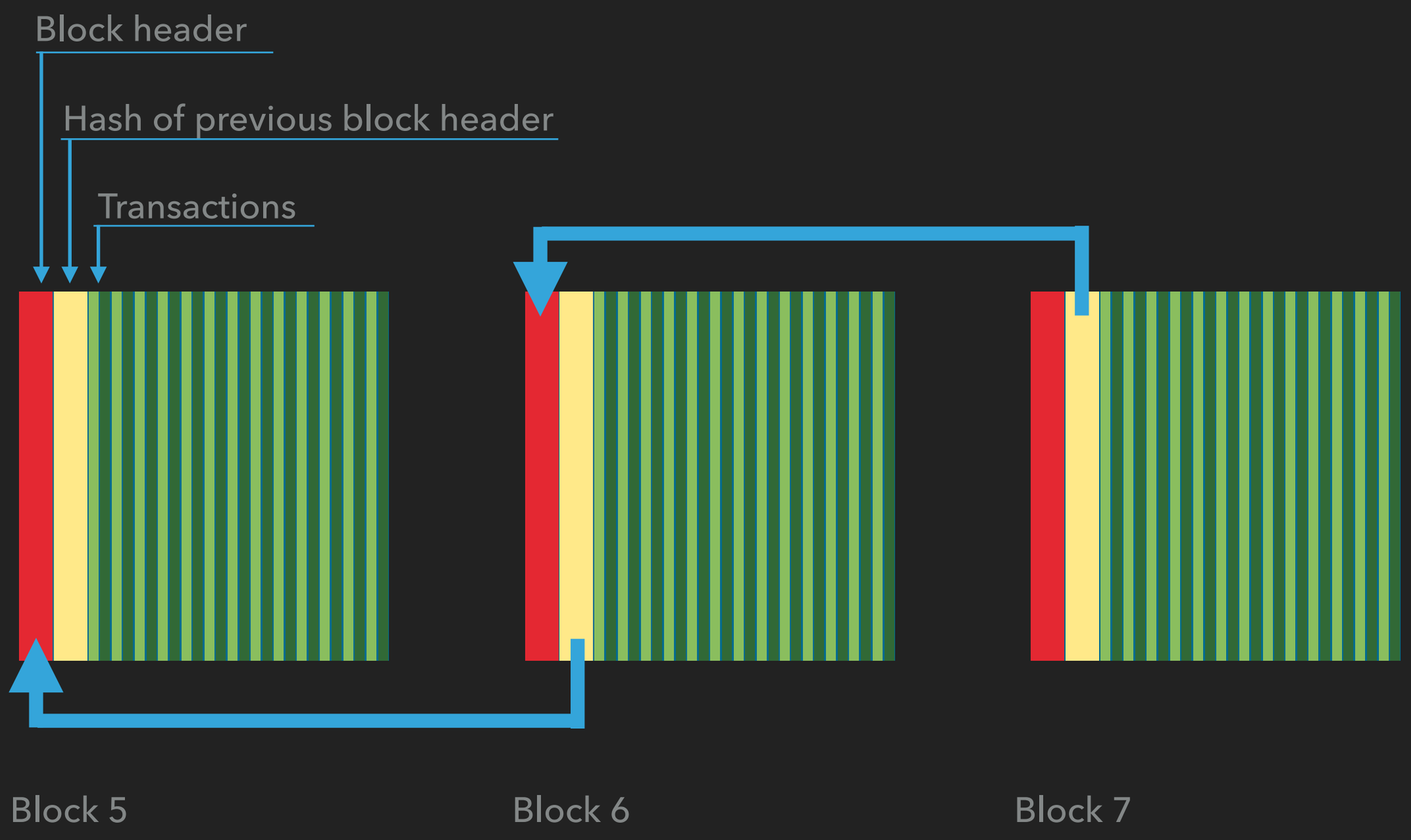
SATOSHI'S SOLUTION: A DISTRIBUTED LEDGER

- A ledger stores every transaction
- The ledger is distributed to everyone running the network
- Everyone has a copy of every transaction
- The majority of the network has to agree on a transaction in order to consider it valid.

THE FIRST BITCOIN TRANSACTION



BLOCK STRUCTURE



#HASHES_ARE_NOT_HASHTAGS

BITCOIN USES

SHA256(SHA256(BLOCKHEADER))

#HASH #DEMO

TRANSACTIONS

- Transactions happen between two bitcoin addresses
- The owner of the sender address creates a transaction
- By signing the transaction with his private key
- Transactions get verified by miners and get added to the next block
- Once the block is completed and propagated to the other nodes, the transaction becomes a fact.

ADDRESSES

- Addresses generated by an algorithm.
- Two keys get generated: a **public key**, which acts as the recipient address. And a **private key**, which proves ownership. The private key must be kept secret.
- Anyone can generate a new bitcoin address, even offline. Even by pen and paper.
- A sender can send to a new address, even if that was generated offline and it never interacted with the network.

WALLETS

- A wallet is just a software that stores the addresses and its private keys
- There are no bitcoins in a bitcoin wallet. Just keys.
- There are no bitcoins even in the blockchain – only transactions. If you have an incoming transactions of 1 BTC and no outgoing transactions, then it is implied that you have 1 BTC

PUBLIC AND PRIVATE KEYS

Public key cryptography is another set of asymmetric cryptographic functions like hashes.

They are called asymmetric, because they only go one way. For example hashing a long string can be done, but recovering the long string from the hash is impossible.

Public and private keys work somewhat similarly.

PUBLIC AND PRIVATE KEYS 2 — GENERATING A TRANSACTION

The sender creates a transaction that says “I want to send x BTC from address A to address B“

The sender signs the transaction with the private key that belongs to address A.

The miners check the signature. Knowing address A, it is trivial to determine whether the sender indeed has the key or not.

MINING

- Mining is the process of confirming transactions
- Miners collect unconfirmed transactions and put them into a new block
- Miners “mine” the block and if the peers accept it, it gets distributed and it becomes part of the blockchain
- For this work, the miners collect the transaction fees and the “block reward” – new bitcoin minted by the network.

IF ITS SO SIMPLE, WHY ARE THERE HUGE MINING FARMS?

MINING AS A COMPETITIVE SPORT

- Fair and random distribution of miners is required.
- Important to fairly compensate miners.
- It would be a security risk if it would be known which miner will mine which block in advance. So it has to be provably random.
- Difficult when decentralized.

BITCOIN MINING IS A DECENTRALIZED LOTTERY

THE MORE COMPUTING POWER YOU HAVE

THE MORE BLOCKS YOU WILL MINE

PROOF OF WORK

- The miners compete in solving a puzzle. When they find the solution, that is the **proof** that they performed the **work**.
- That gives them the privilege to creat the block and collect the fees.
- The work and the proof is another asymmetric algorithm example – very difficult to find the solution, but very easy to verify.
- There are other types of “proofs”. More later.

CONCLUSION

BITCOIN, THE FIRST KNOWN BLOCKCHAIN SYSTEM WAS CREATED TO SOLVE THE DOUBLE SPENDING PROBLEM IN DECENTRALIZED SYSTEMS.

PRIVATE KEY

PUBLIC KEY

ADDRESSES

TRANSACTIONS

WALLETS

THE BLOCKCHAIN IS

TRANSACTIONS ORGANIZED INTO BLOCKS

CHAINED TOGETHER BY HASHES

THERE ARE NO BITCOINS IN A BITCOIN WALLET

ONLY PRIVATE AND PUBLIC KEYS

THERE ARE NO BITCOINS ON THE BLOCKCHAIN

ONLY TRANSACTIONS

THE MINERS ARE THE TRANSACTION VALIDATORS.

THEY GET THE PRIVILEGE TO CREATE A NEW BLOCK BY PARTICIPATING IN AND WINNING A DISTRIBUTED LOTTERY.

THANK YOU

TWITTER, MEDIUM: @AKOMBA, EMAIL: A@AKOMBA.COM