Block-Chain Bitcoin Fundamentals

Monetary and Financial Architectures

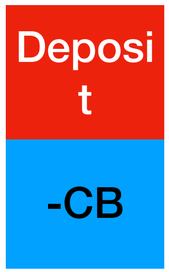
Saki Bigio

Bitcoin - The Starting Point

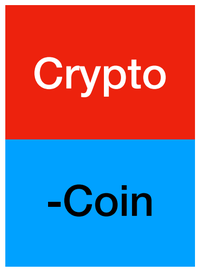
- Bitcoin was an idea released in a paper by an anonymous author, Satoshi Nakamoto
- Since then, there have been multiple crypto-currencies launched:
  - Litecoin
  - Ripple
  - Ethereum
  - Ethereum Classic

Parallel - Traditional Finance

Parallel - Traditional Finance



- Bank & CB verify transaction
  - System relies on trust of financial institutions, CB

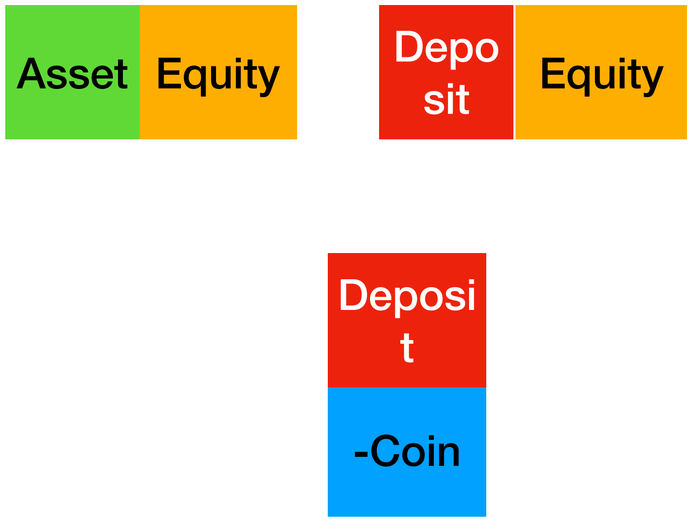


- No Centralized Party verifies transaction
- System relies on common acceptance, reward system

Parallel - Traditional Finance

- You want ability to Exchange

Parallel - Traditional Finance

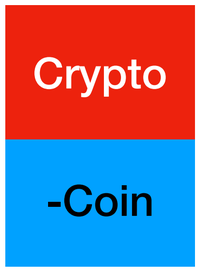


- Issue #1: You want to make sure you are the one who transferred funds
- For that, you either use your credit card (Pin) and you sign your card

Parallel - Traditional Finance

- System is Electronic
- Could easily forge any Bitmap (of signature)
- Crypto Transactions rely on Digital Signatures

- Digital Signature
- Public Key: PK
- Secret Key: SK



- Digital Signature: 256 Bits

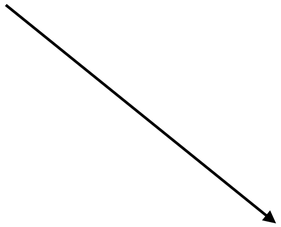
Bitcoin - Verification

- SIGN (“Message”, sk)=SIGNATURE (256 digits)
- VERIFICATION(“Message”,SIGNATURE,pk)=True/False

- Message:
- Alice Pays Bob 50 Bitcoin
- Alice Signs (SIGN)
- Anyone can verify (did Alice sign message?)

Bitcoin - Verification

- SIGN (“Message”, sk)=SIGNATURE (256 digits)
- VERIFICATION(“Message”,SIGNATURE,pk)=True/False

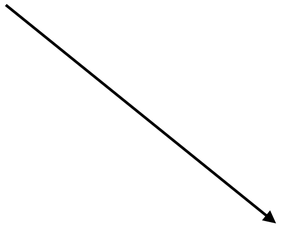


- Message:
- Alice Pays Bob 50 Bitcoin
- Alice Signs (SIGN)
- Anyone can verify (did Alice sign message?)

Leap of Faith:
Cryptographers: study methods of encryption
SIGNATURE is such that impossible to have TRUE in VERIFICATION without guessing SK
You would require, near 40 the life of Universe to Guess with Current Machines

Bitcoin - Verification

- SIGN (“Message”, sk)=SIGNATURE (256 digits)
- VERIFICATION(“Message”,SIGNATURE,pk)=True/False

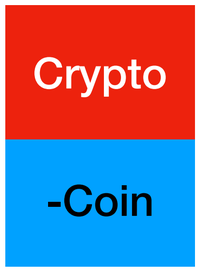


- Message:
- Alice Pays Bob 50 Bitcoin
- Alice Signs (SIGN)
- Anyone can verify (did Alice sign message?)

Leap of Faith:
Cryptographers: study methods of encryption
SIGNATURE is such that impossible to have TRUE in VERIFICATION without guessing SK
You would require, near 40 the life of Universe to Guess with Current Machines

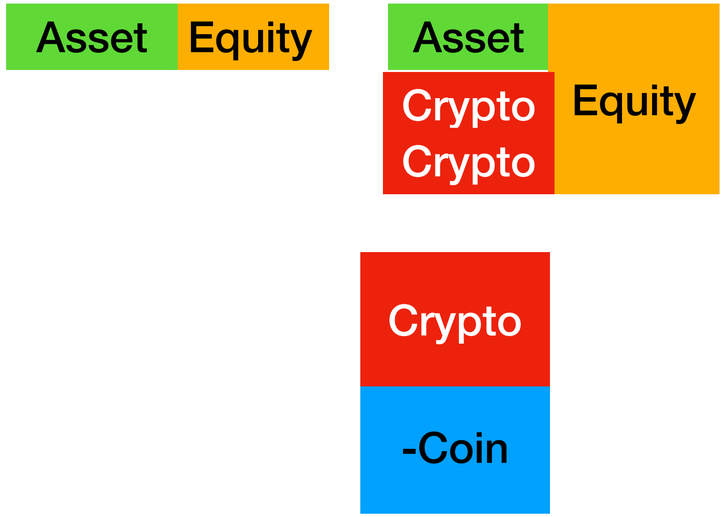
Parallel - Traditional Finance

- System is Electronic
- Could easily DOUBLE COUNT TRANSACTION
- ONLY Crypto transfer registered ONLY



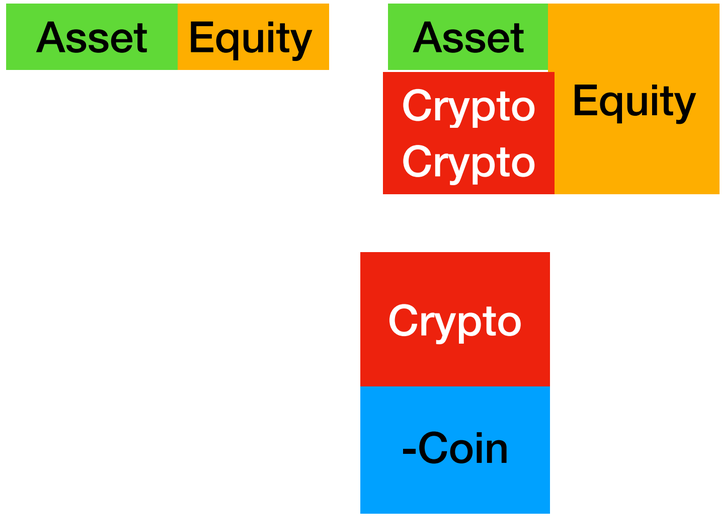
Parallel - Traditional Finance

- System is Electronic
- Could easily DOUBLE COUNT TRANSACTION
- ONLY Crypto transfer registered ONLY
- What Prevents this?
- Key: each transfer has a unique ID.
- It will attach a single value



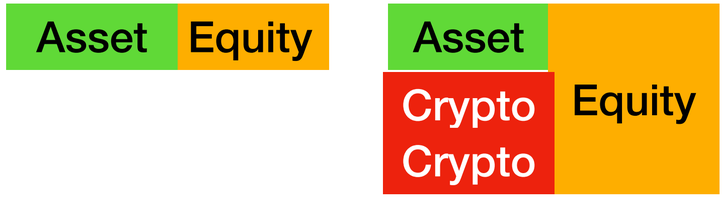
Parallel - Traditional Finance

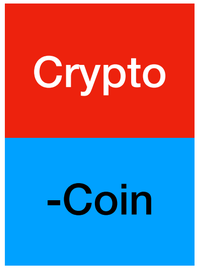
- System is Electronic
- Could easily DOUBLE COUNT TRANSACTION
- ONLY Crypto transfer registered ONLY
- What Prevents this?
- Key: each transfer has a unique ID.
- It will attach a single value



Parallel - Overdraft Problem

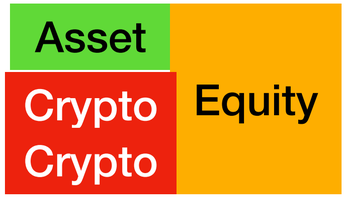
What about overdraft?
Who keeps information on account balance?
We need to verify all past History of Transactions!

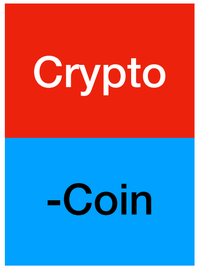




Parallel - Overdraft Problem

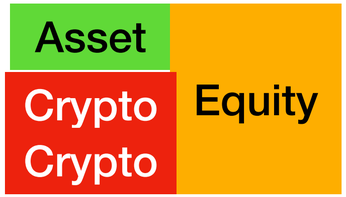
Solution is: Blockchain
Common Ledger: Keeps History of Every Transaction Ever Done
Seems like a lot of information to store.
Also, it would need to be stored in only one place (CENTRALIZED LEDGER)
What Block-Chain does is it Broadcasts Information to anyone interested
Everyone in System has their own Ledger.
PROBLEM: Why do we agree?

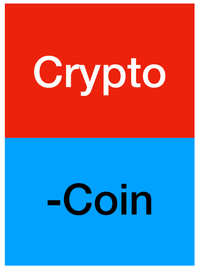




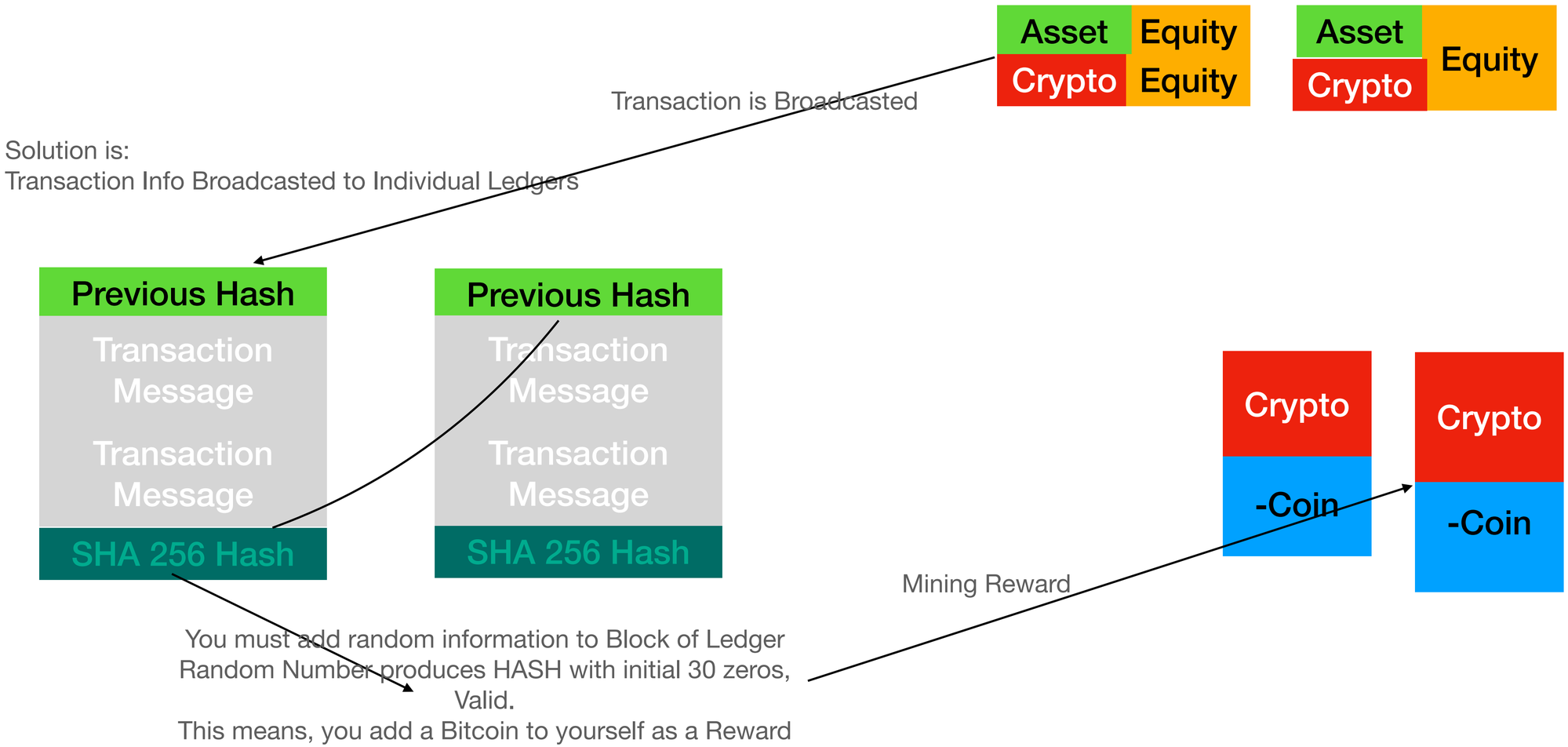
Parallel - Verification of Transactions

Solution is: PROOF OF WORK
USE of SHA256 Function
(Hash Function)
Idea: you have to search randomly with computer power for
Sequence of 30 zeros prior to attaching zeros to a message.
Broadcast (BLOCK) is only CONSIDERED VALID after SUCCESFUL Proof of WORK
BLOCK: Set of Transactions
BLOCK: ALSO CONTAINS HASH OF PREVIOUS LEDGER
QUESTION: DO WE NEED TO KEEP TRACK OF ALL THE HISTORY LEDGER?
    - I think we can descentralize it.
- Any manipulation of block chain, would require all of the proof of work, to verify the transaction
- POW



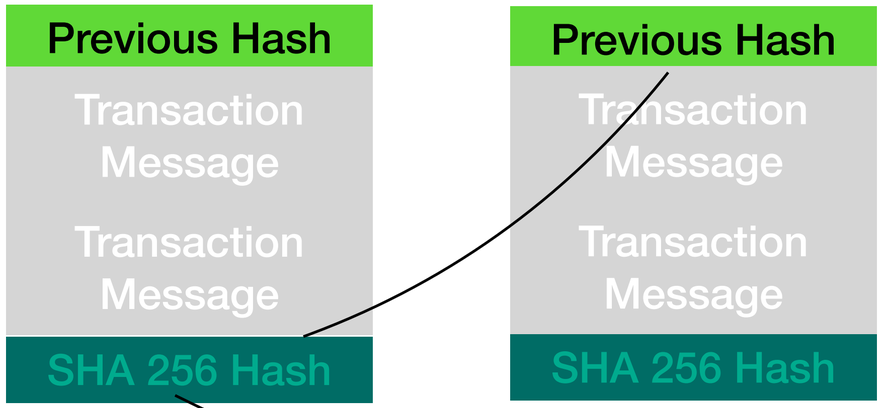


Public Ledger - Proof of Work



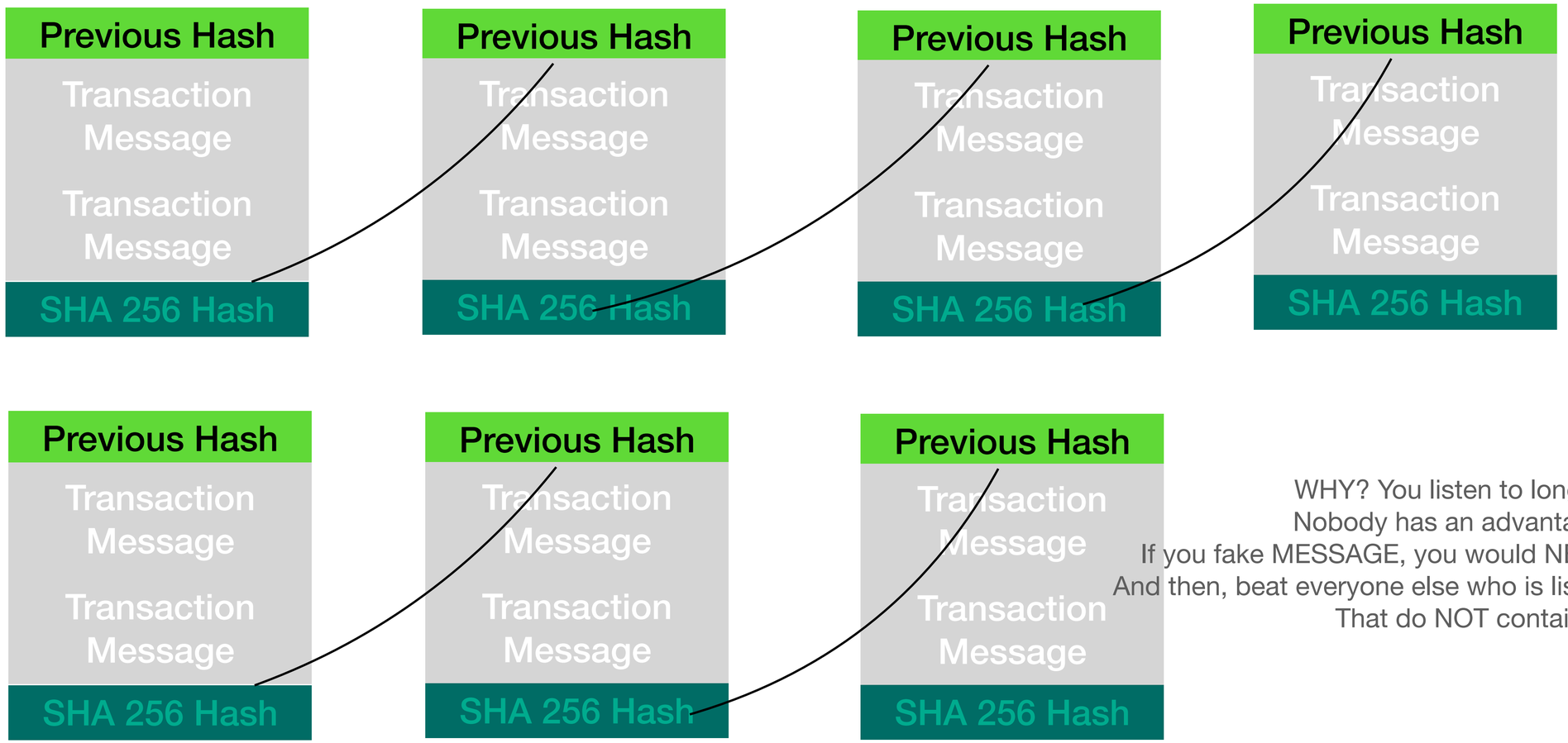
Public Ledger - Which Block Chain to Accept?

Solution is:
Miners are broadcasting blocks.
What prevents them from broadcasting blocks that say:
“Pay Saki 1’000’000” in Crypto?



You must add random information to Block of Ledger
Random Number produces HASH with initial 30 zeros,
Valid.
This means, you add a Bitcoin to yourself as a Reward

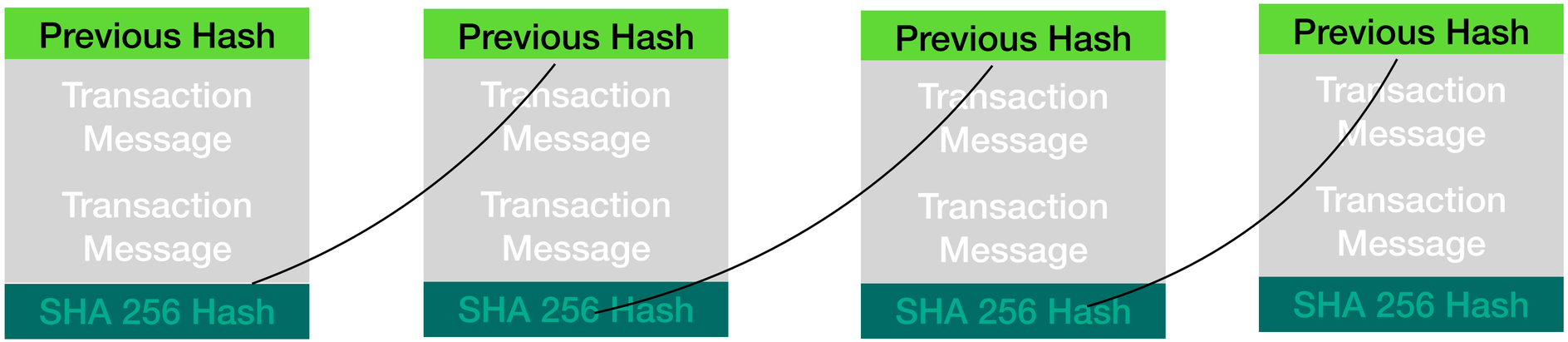
Public Ledger - Which Block Chain to Accept?



WHY? You listen to longest chain because
Nobody has an advantage in computation.
If you fake MESSAGE, you would NEED to create a HASH (COSTLY)
And then, beat everyone else who is listening and adding items to chains
That do NOT contain fake message

Protocol: Always listen to longest chain.

Public Ledger - Which Block Chain to Accept?



DESCENTRALIZED: EXCHANGE! Brilliant IDEA!

Summary of Concepts

Digital SIGNATURE
LEDGER IS CURRENCY
DECENTRALIZED CONSENSUS | LEDGER
BLOCK CHAIN
PROOF OF WORK

Proof of Work - More Detail

TIME: 10 minutes to Verify
As you add miners LINEARLY, it BECOMES INDIVIDUALLY harder to MINE
Keeping time to FIND Hash, roughly stable

TIME: Cryptos Differ by TIME
BITCOIN: 10 Minutes
ETHEREUM: 15 s
XRP: 3.5 s
LTC: 2.5 m

Rewards: DROP AS SYSTEM GROWS
(SEE BLOOCK EXPLORER)
09-12: 50 COINS
12-16: 25 COIN
16-20: 12.5 COINS
20:24: 6.25 COINS
24:28: 3.125 COINS
23:32: 1.5625 COINS
32:36 1 COIN
NO MORE

LIMIT SUPPLY OF COIN!

FEES

Instead of rewarding in coin, you can pay a small fee in the transaction.
Thus, you can pay your friend, and pay the broadcaster that finds the Hash.
The longer the chain, the broadcaster will collect more and more fees.

SMART CONTRACT

We now move to second slide.

CONCEPTS:
STABLE COINS
ORACLES
dApps
Non-Fungible Tokens (NFT)