Ethos

What is Bitcoin?

bitcoin

What You Will Learn

- What is Bitcoin?
- What is a blockchain?
- How do transactions work?
- How does mining work?

We won’t go into any code, but we will dig into a lot of the concepts in good detail! This lecture is a bit longer than others, but by the end you will be very familiar with Bitcoin.

Ethos

Ethos

What is Bitcoin?

Bitcoin is the first and most popular cryptocurrency. Founded by the anonymous Satoshi Nakamoto in 2009, it has launched a lot of innovation in blockchain technology which underpins its network.

What is the blockchain?

- Massive shared ledger of transactions
  - All transactions on the network get recorded
- Has “blocks” that get created at certain intervals which contain data
- Blockchains are “append only” so they only get larger over time

As of July 2017, the full Bitcoin blockchain was about 126 GB

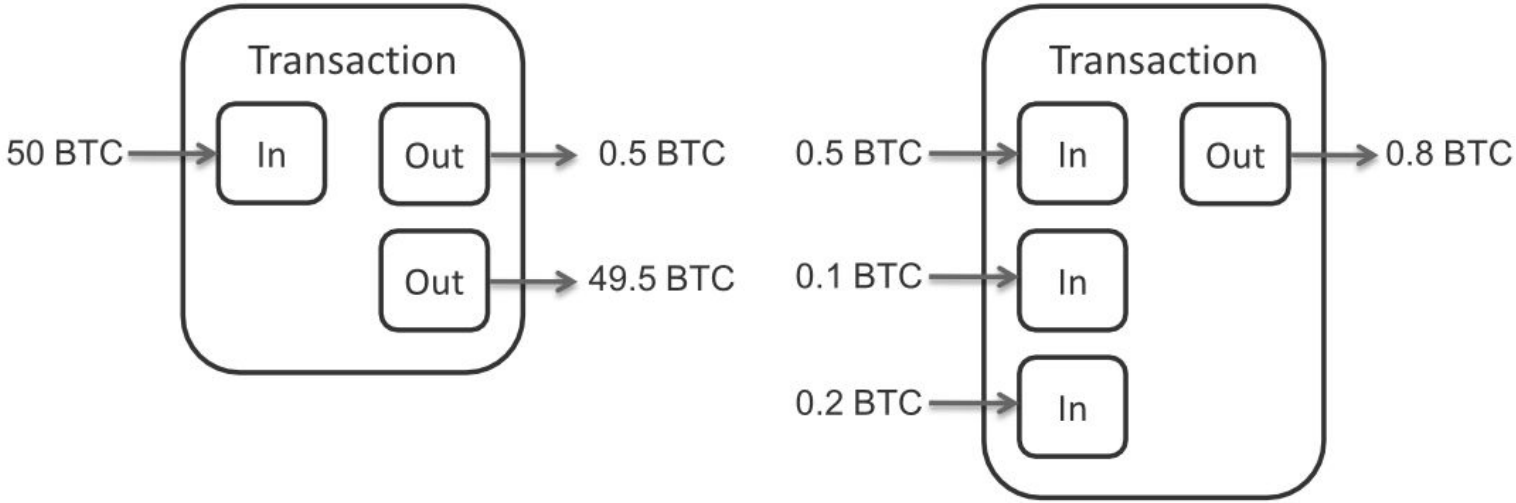
Ethos

Bitcoin Blockchain Implications

- Transparent transactions (on Bitcoin at least)
  - Every person has a copy of every transaction
- Block explorers like blockchain.info allow you to view blockchain data
- Every transaction has a unique ID that can be referenced

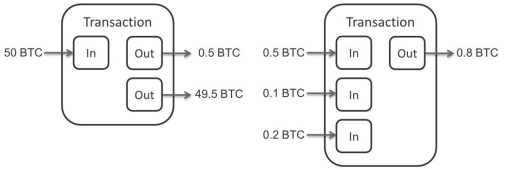
You can see the balance and past transaction history of any address!

How does a transaction work?



This is a visual representation of a transaction. The first shows a single input with multiple outputs while the second shows multiple inputs with a single output.

How does a transaction work?



- Bitcoin works with inputs and outputs
  - When you receive Bitcoin you receive an input to your address
  - When you send Bitcoin, you are using outputs to your address to send an input to another address
- Transactions send unspent outputs as inputs to another address
  - Your balance is the sum of all unspent outputs
- To send a transaction, you use your wallet's private key to sign a transaction with an output and an amount
  - Signed transactions can only send the exact amount to the address specified and nothing else!
  - This is what keeps the network secure since you never need to expose your private key

Wallet software handles the transaction signing for you and broadcasts only signed transactions. You can give signed transactions to anyone and signed transactions are what is stored on the blockchain

Ethos

Ethos

What is Bitcoin mining?

Mining is the process by which transactions get added to the blockchain. Mining also ensures that transactions are valid and that nobody is creating a fraudulent chain through proof of work.

What is Bitcoin mining?

- Miners verify transactions, bundle transactions into blocks then solve the proof of work
  - The miner who solves the proof of work creates and issues a valid block to the network (More on proof of work in next slide)
  - After solving the proof of work, the miner gets an unspent output for themselves as a reward
- The mining process ensures that nobody is trying to spend an invalid output (i.e. that they actually have the inputs required to create the outputs)
- Miners have a lot of checks on transactions to ensure their validity

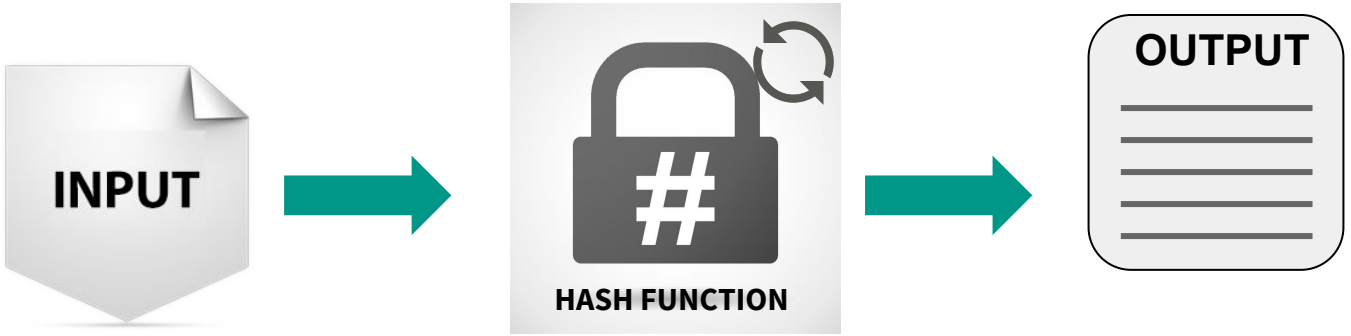
For a full list of everything that miners check, see https://en.bitcoin.it/wiki/Protocol_rules#.22tx.22_messages

Ethos

What is Proof of Work?

Proof of work uses a one-way hash function

A one-way hash functions has the property that given a “question” it always produces the same “answer” - but given only the “answer” it is impossible to know what the “question” was.



Example: ***Dog***

SHA-256
(what Bitcoin uses
as its hash function)

0eb129bf94594aae
ee66e38361d7be21
2cd927c3df4dd92e3
ded2e0da0c7ad88

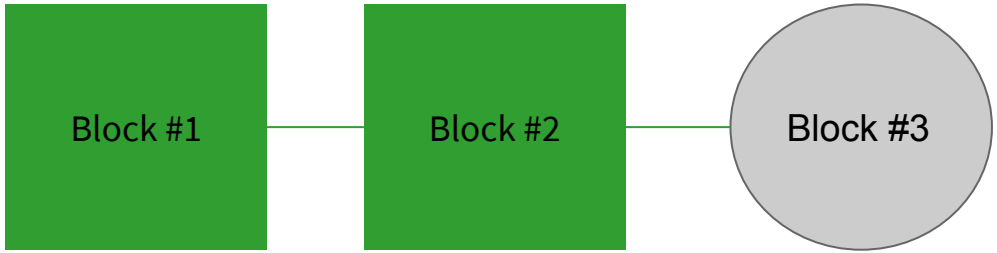
Ethos

What is Proof of Work?

- Using the one-way hash function, Proof of Work is the process by which miners prove they did work
- Miners “ask questions” using this function extremely quickly trying to get a result from the function within certain parameters
    - Example: Only hashes where the first 7 digits are 0s will be accepted
- This is why when a new block is created, a lot of computational work was put into it
    - Example: Whoever finds an input that creates a hash with 7 leading 0s will have “solved” the puzzle
- Furthermore, the “question” you give the function has to include the previous block’s “answer” creating a “blockchain”
    - As part of your input you have to include the previous block’s hash
    - If you want to reverse a transaction, you will have to undo all the blocks that came after that transaction as well which means a lot of computation

Visualization of Mining Process

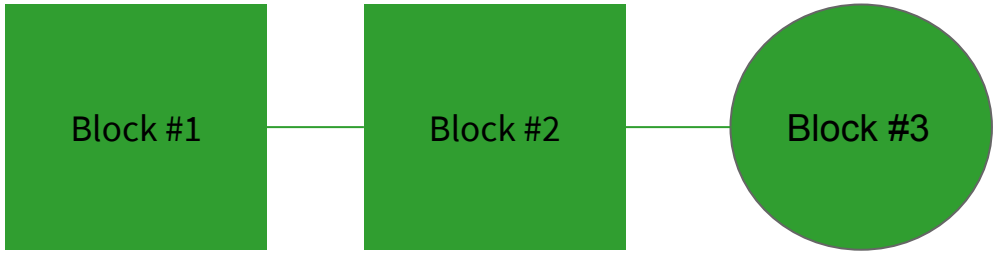
Miners Searching for the next block…



Ethos

Visualization of Mining Process

Block is found + proof provided



00000000839a8e6886
ab5951d76f411475428
afc90947ee320161bbf
18eb6048

000000006a625f06636
b8bb6ac7b960a8d037
05d1ace08b1a19da3f
dcc99ddbd

Found!

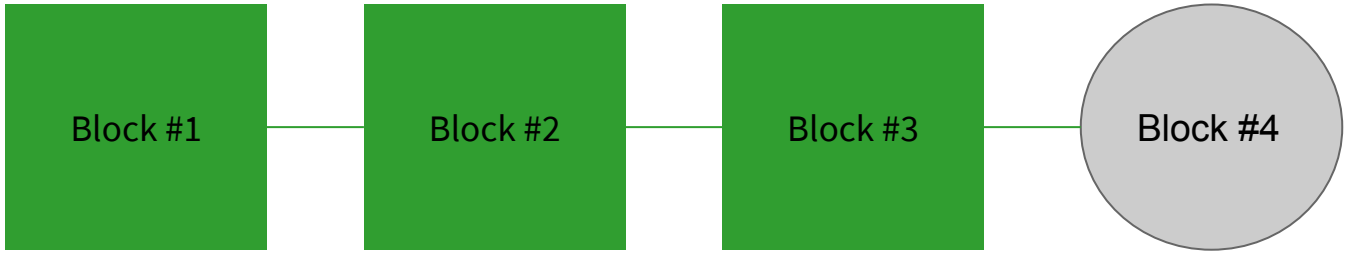
0000000082b5015589
a3fdf2d4baff403e6f0b
e035a5d9742c1cae62
95464449

Proof of Work: 1844305925
(Nonce Value)

Ethos

Visualization of Mining Process

If the block is accepted, then miners begin mining using block #3's hash



00000000839a8e6886
ab5951d76f411475428
afc90947ee320161bbf
18eb6048

000000006a625f06636
b8bb6ac7b960a8d037
05d1ace08b1a19da3f
dcc99ddbd

Accepted!

0000000082b5015589
a3fdf2d4baff403e6f0b
e035a5d9742c1cae62
95464449

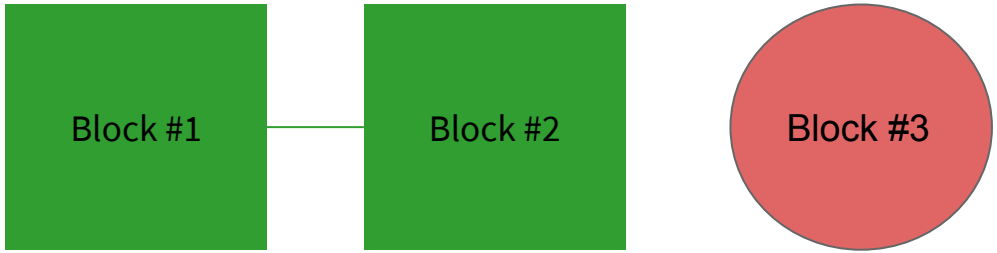
Proof of Work: 1844305925
(Nonce Value)

Searching...

Ethos

Visualization of Mining Process

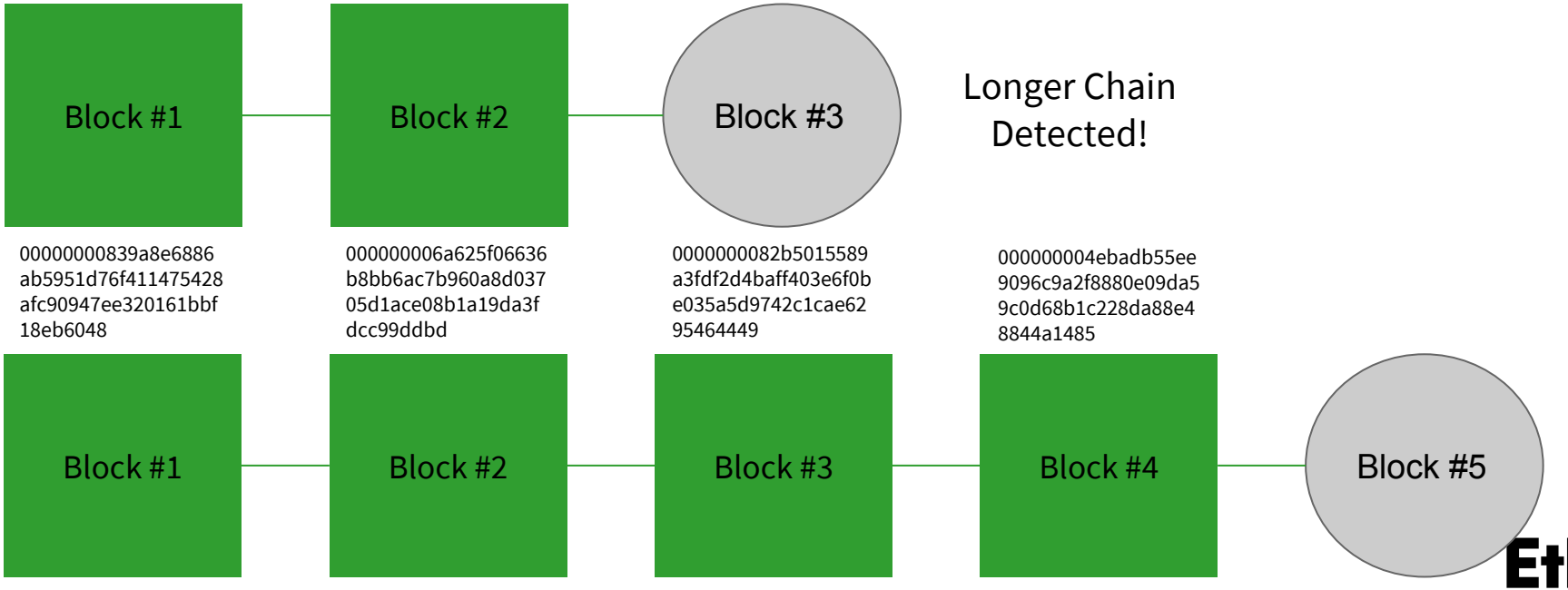
If block is rejected (perhaps invalid proof of work) miners will continue mining on block #2's hash



Ethos

Visualization of Mining Process

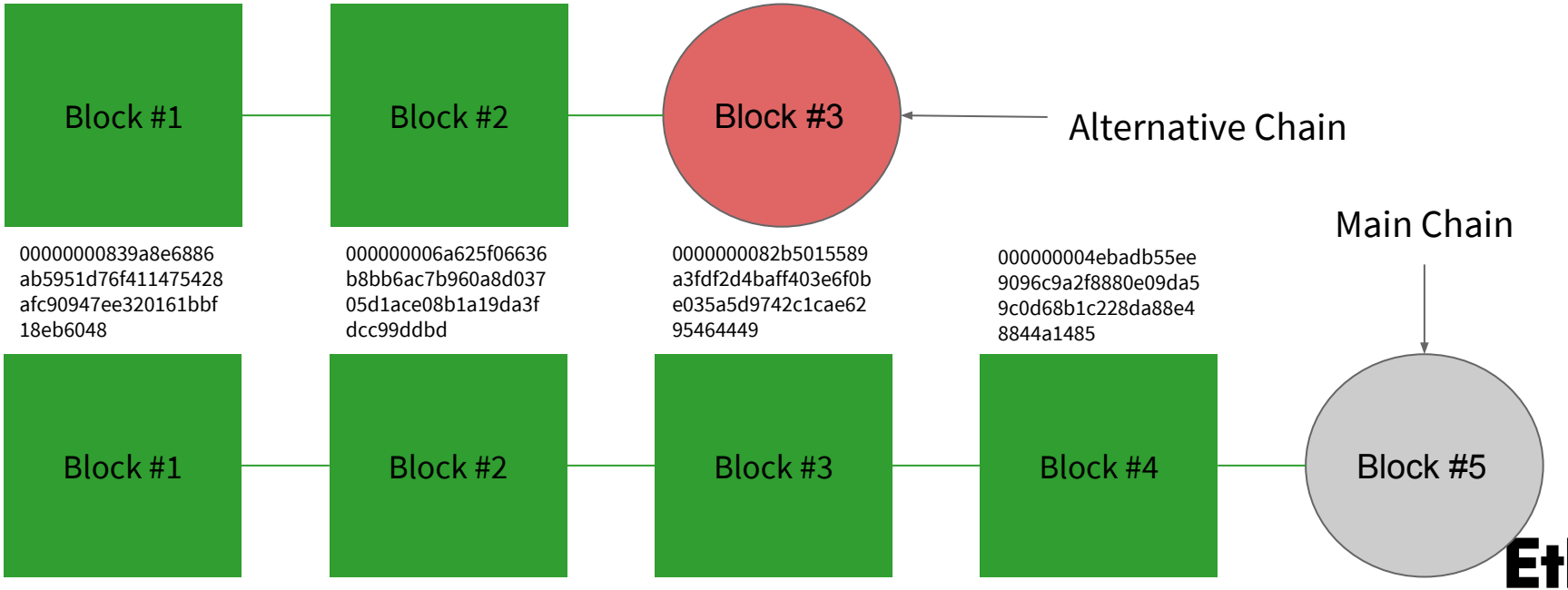
In consensus, the longest chain always wins since it has more work. This makes it very difficult to create a fraudulent chain. If a longer chain is detected, miners switch to that chain.



Ethos

Visualization of Mining Process

Additionally, blocks mined on a shorter chain are “orphaned” blocks. They could have been valid, but were not mined into the main chain. Also if a block is rejected, then it isn’t included in the main chain.



Ethos

Ethos

Mining of some sort is essential for every blockchain based currency

What Mining Enables

- Confirms transactions
- Allows value to be transferred
- Secures and ensures no malicious parties attack the network
- Creates Blockchain “Repository of Truth”
- Underpins trustless consensus
- Allows Bitcoin and other currencies to work

Ethos

What is Bitcoin?

bitcoin