Block Chain

Rohit Musti

CUNY - Hunter College

March 30, 2022

Table of Contents

Disclaimer

- These slides do not reflect my personal opinion on the viability or effectiveness of blockchain technology or cryptocurrencies
- Please carefully review any investments into cryptocurrencies and make sure you have an extremely clear understanding of why you believe that investment will yield a significant enough return to justify the risk of it failing
- There are many fraudulent scams out there trying to take your money through cryptocurrency schemes and a few honest actors trying to do what they believe is right. At times it can be hard to distinguish them
- I am also (at the time of this slide creation) not personally invested in any blockchain technologies so I don't have any financial incentive to see these new ways of transacting succeed. If that changes, this slide will be updated.

2 Overview

Blockchain

- *definition*: a persistent, transparent, public, append-only ledger that is managed using a mechanism that allows distributed group of actors to work together to verify the ledger and new additions without trusting one another and such that no one actor can dominate who controls the ledger
- *use*: to allow a group of actors that do not inherently trust one another to have a mechanism for confirming that transactions did in fact happen
- this isn't inherently limited to just transactions, theoretically any digital exchange of information can be put on a distributed ledger like this

Why?

- Let's pretend we cannot trust institutions
- For example, what if you learned in a cryptography class taught by a very cool professor that the US government has, throughout its history, actively tried to undermine the cyber security of its citizens (cough cough NSA)
- What if, Wells Fargo was found guilty of employees opening up fake accounts in customers names, signing them up for credit cards, forging their signatures, and secretly transferring the customers money without their permission between 2002 - 2016. What if this very same bank was found guilty of charging mortgage customers unnecessary fees and forced auto-loan borrowers to buy unnecessary insurance.

Why?

- If we cannot trust institutions to safely handle our transactions, we need to hold them accountable through the mechanisms we have agreed up on socially (courts, laws, regulators, etc.).
- If those mechanisms fail, we either need to revise those systems or overthrow those in power
- Systemic change is hard in most western countries and revolutions tend to be bloody and violent, so having our own mechanism for transferring and maintaining money would be incredibly valuable. This is the central argument for crypto-currencies.

3 Mechanisms

Distributed Ledger: Example

- If you exchange money with your friends, exchanging cash or venmo/zelle-ing all of the time is inconvenient. So you might keep a ledger to keep track of who owes who what money (kind of like a bar tab).
- Every so often, you calculate how much money you spent vs received. If you spent more than you received, you put money in the pot. If you received more than you spent, you take money from the pot.

Distributed Ledger: Weak Protocol

1. Anyone can add lines to the ledger.
2. At the end of a time period (every two weeks, money is exchanged based on the ledger record)

Distributed Ledger: Weak Protocol Weaknesses + Solutions

1. Anyone can add lines to the ledger, therefore Bob could write *Alice owes bob $100* without Alice having sent Bob $100
2. Solution: Unique Ids + Digital Signatures. If messages have unique ids you cannot replicate them without changing the ids and if Alice signs all transactions with a digital signature, then we can guarantee that the transaction came from the person controlling her secret key.
3. Is this actually the same as Alice sending it? No. What if she leaves her secret key at a coffee shop or someone guesses it?

Distributed Ledger: Weak Protocol Weaknesses + Solutions

1. Anyone can add lines to the ledger
2. At the end of a time period (every two weeks, money is exchanged based on the ledger record)
3. Only signed, unique ID transactions are considered valid

Distributed Ledger: Weak Protocol Weaknesses + Solutions

1. What if someone refuses to settle up cash?
2. What if they send hundreds of dollars at a time to people and then refuse to actually pay up when the time period ends.
3. Introduce a mechanism to stop someone from spending money that they do not have. (maybe at the begining of the time period everyone has to add money to their account that serves as their account total and this is recorded on the ledger too)

Distributed Ledger: Weak Protocol Weaknesses + Solutions

1. Anyone can add lines to the ledger
2. At the end of a time period (every two weeks, money is exchanged based on the ledger record)
3. Only signed, unique ID transactions are considered valid
4. No overspending.

Distributed Ledger: Weak Protocol Weaknesses + Solutions

- Who controls the ledger document?
- you distribute it, everyone gets their own copy of the ledger
- Once a transaction happens, it is broadcasted and everyone else records that transaction
- In order to verify that a transaction actually happened, you would want to know that everyone else received the very same transaction.
- How can we guarantee that everyone else is receiving the same transactions and recording them correctly? This is the problem solved in the original Bitcoin white paper

Distributed Ledger: Trust

1. How can we guarantee everyone is recording the same transactions?
2. You trust the ledger that has had the most computational work put into it
3. Specifically, we append a number to the end of a block of transactions such that if you take the SHA-256 hash function of those messages with that number appended at the end, you get a resulting hash where the first 30 digits are zeros (number of zeros increased to keep total time to compute a block to around 10 minutes).
4. This allows us to guarantee that whoever computed the hash function put in an enormous amount of work because they had to essentially brute force until they got that number. This is "proof of work".

Distributed Ledger: Trust

1. Organize ledger into a series of blocks
2. Each block needs to have this proof of work number tacked on the end to be valid

Distributed Ledger: Ordering

1. Blocks need to be in order though! What if these blocks are verified with proof of work but don't have any ordering. No way to determine if overspending
2. Therefore, each block has to contain the previous block's hash output in its header
3. this results in the "block chain"

Distributed Ledger: Mining

- In order to incentivize block creators to compute these hashes, we have to allow them to prepend a transaction to the top of every transaction giving them some kind of currency total
- What miners do is they listen for transactions, create blocks, broadcast blocks, and get rewarded for this little lottery.
- If you want to make transactions, what you do is you listen for miners broadcasting blocks and add it onto your chain. If there are two conflicting blocks, then you take whicheveryone is part of the longest pre-existing chain, ties are broken by whichever one is made longer next
- Despite there being no centralized authority, whichever blockchain has the most work into it, is the longest,
- Also, the reward for computing a block decreases by half every 210 thousand transactions so there will never be more than 21 million bitcoin in existence

Longest Chain Security

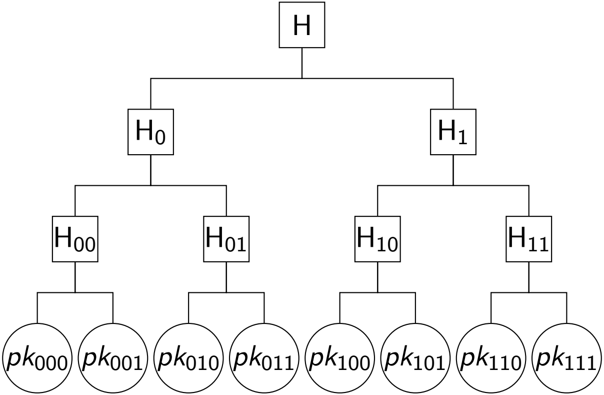
- Let’s say you alter a transaction in a block you receive as a miner to trick one person into thinking you sent them money and make everyone else not know (i.e. you send them a fraudulent block)
- You would have to keep sending that person new blocks based on your fraudulent block. At some point you will fall behind the rest of the miners and will not be able to keep beating them
- Unless you have around half the computer power of the entire chain, then you will quickly fall behind everyone else
- In general, you shouldn’t trust a new block immediately, you want to trust it every it has a sufficient number of blocks after it

Flaws

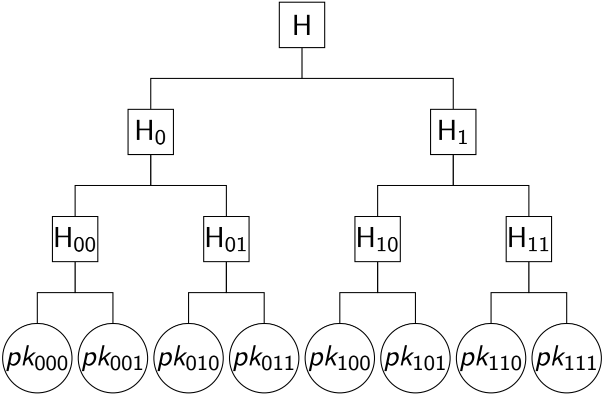
- Bitcoin blocks are restricted to 2,400 transactions and a new block is computed roughly every ten minutes, by comparison VISA can handle 24 thousand a second
- Miners also prefer transactions that give them a transaction fee/tip ontop of their regular reward, this means that the transaction fee to get into that 2,400 transaction block is going to go up over time
- blockchain is growing in size infinitely

4 Merkle Trees

Merkle Tree


H
H_0
H_1
H_{00}
H_{01}
H_{10}
H_{11}
pk_{000}
pk_{001}
pk_{010}
pk_{011}
pk_{100}
pk_{101}
pk_{110}
pk_{111}

Merkle Tree


H
H_0
H_1
H_{00}
H_{01}
H_{10}
H_{11}
pk_{000}
pk_{001}
pk_{010}
pk_{011}
pk_{100}
pk_{101}
pk_{110}
pk_{111}

SHA-256