

Bitcoin

ECON 4905

Eric Schulman

Introduction

Introduction

Outline

- Introduction
- Public Ledger
- Mining
- Implications
- Questions

Introduction

What is currency?

- Currency is a store of value
 - The price doesn't fluctuate that much
- Currency is a medium of exchange
 - If I give you currency, you will give me chocolate in exchange
- Some examples:
 - US Dollar
 - Euro
 - Bitcoin?

Introduction

What is Bitcoin?

- Bitcoin is an online currency
 - Each costs ~375 USD
- If you have a Bitcoin you have:
 - Public key (username)
 - Private key (password)
- Might want to use a Wallet
 - Software keeping track of your public and private keys
- May want to print them out
 - If you lose your private key, you lose your Bitcoin!



Introduction

Unsatisfying explanation

- Raises more questions than answers
 - Why can't I recover my username and password?
 - What do you mean by online currency?
 - How does it work?
- We must explore 2 concepts to answer these questions:
 - Public Ledger
 - Mining

Public Ledger

Public Ledger

Bitcoins are a ledger

- There are no Bitcoins!
- Bitcoins are just spots in a ledger
- Your username and password prove you own a spot
- Spots are divisible to 10^{-8}
 - Called a “Satoshi”
- Every time a transaction happens, the ledger is updated

Ledger 0	
Bitcoin 1	Adam
Bitcoin 2	Bonnie
...	...

Ledger 1	
Bitcoin 1	Adam
Bitcoin 2	Adam
...	...



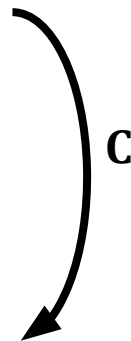
Public Ledger

Intermediation

- We need an intermediary to update the ledger
- We pay this intermediary for updating the ledger by giving them Bitcoin
- Banks work this way
 - Banks are a centralized intermediary for financial transactions

Ledger 0	
Bitcoin 1	Adam
Bitcoin 2	Bonnie
...	...

Ledger 1	
Bitcoin 1	Adam
Bitcoin 2	Adam
Bitcoin 3	Craig
...	...



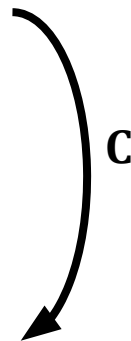
Public Ledger

Decentralization

- Problem:
 - Trusting an intermediary is difficult because they can lie
 - They can manipulate the ledger to benefit themselves
- Solution:
 - Let's make the ledger public!
 - Anyone can be an intermediary
 - If you lie in the ledger, it can be corrected

Ledger 0	
Bitcoin 1	Adam
Bitcoin 2	Bonnie
...	...

Ledger 1	
Bitcoin 1	Craig
Bitcoin 2	Craig
Bitcoin 3	Craig
...	...



Public Ledger

Still more questions...

- Why would the people updating the ledger agree on one ledger?
 - There shouldn't be two list of Bitcoin transactions; there should be one
- Why don't the people update the the ledger collude with each other against the people who don't?
 - Not every Bitcoin user wants to update the ledger
 - Those who update the ledger should be competing with each other
- To understand how Bitcoin addresses these issues we must understand mining

Mining

Mining

What is Mining?

- Mining is the process by which the Bitcoin ledger is updated
- Those who update the ledger are called miners
- Miners can earn a limited opportunity to manipulate the ledger
 - Miners can add 25 spots to the the ledger per update paying themselves
 - The opportunity happens at a decreasing rate
 - Rules are based on the Bitcoin protocol
- Mining involves 3 concepts:
 - Blockchain
 - Hashing
 - Proof of Work

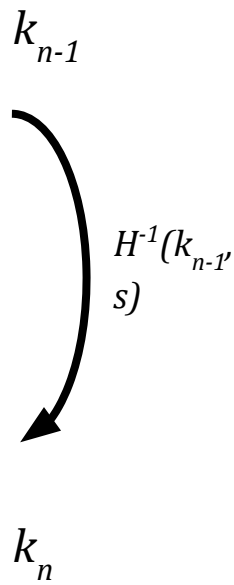
Mining

Blockchain

- The Blockchain is a chain containing current ledger and the ledger's transaction history
- The current state of the ledger is linked to its history, so miners collaborate

Ledger n-1	
Bitcoin 1	Adam
Bitcoin 2	Bonnie
...	...

Ledger n	
Bitcoin 1	Adam
Bitcoin 2	Adam
Bitcoin 3	Craig
...	...



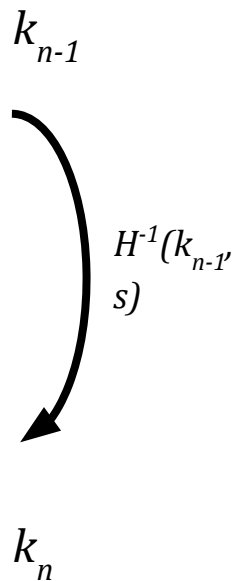
Mining

Blockchain

- Let's call each "ledger" a "block"
- Let updating the ledger be a function H^{-1}
 - For block k we compute:
 - $H^{-1}(k_{n-1}, s) = k_n$
- Each miner tries to find the next block
- This calculation is dependent on the result of the last "block"

Ledger n-1	
Bitcoin 1	Adam
Bitcoin 2	Bonnie
...	...

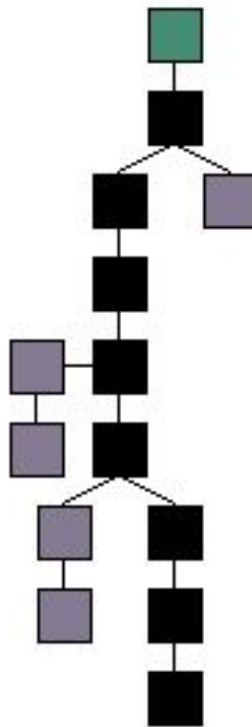
Ledger n	
Bitcoin 1	Adam
Bitcoin 2	Adam
Bitcoin 3	Craig
...	...



Mining

Blockchain

- Why do miners work together on one Blockchain?
 - Miners agree the longest chain is correct
 - Bitcoin mined in other chains are not accepted
- The longest chain grows faster than the other chains
 - The majority of the network's computing power is devoted to it
 - Vulnerable to 51% attack



Mining

Hashing

- Why don't miners collude on the Blockchain?
- Updating the Blockchain requires completing a computation called a hash
- Hashes are easy to check, hard to solve
 - Checking a hash computation i.e. $H(k) = s$ takes $O(1)$ time i.e. short
 - Computing a hash i.e. $H^{-1}(s) = k$ takes $O(n!)$ time, where n is the size of s i.e. long
- Only one person can complete each hash
- Miners only can only manipulate the ledger after completing a hash
 - This is when they get paid in new Bitcoin when they complete a hash
 - Easily verifiable

Mining

Metaphor: Opening a Safe

- Very easy if I know the password
- Very difficult if I don't
 - I must try every possible password
- For “safe” s and “key” k when I try a password I'm computing $H(k) = s$
 - I only need to compute this once
- When I try guess the password I'm computing $H^{-1}(s) = k$
 - If k is n digits long I must try $n!$ passwords.



Mining

Proof of Work

Problem:

- How do I know who completed each hash first?
 - Once you open the “safe” you must announce the key so others can verify it
 - Now everyone knows the key!

Solution:

- Proof of work
 - Prove you solved it first
 - Using the safe metaphor: Write down all the passwords you’ve tried
 - Doing the computation takes the same amount of time to copy

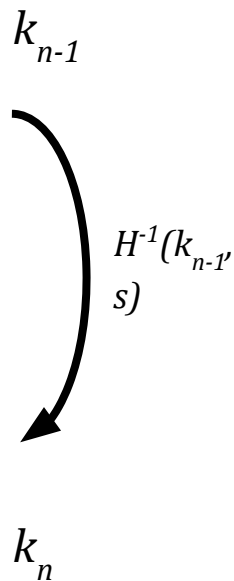
Mining

Putting it all together

- Each hash is dependent on the hash before it
- Miners only get Bitcoin for being the first to complete each hash
- Miners agree on the longest chain of hashes called the Blockchain
- Each hash requires a proof of work to prove you solved it

Ledger n-1	
Bitcoin 1	Adam
Bitcoin 2	Bonnie
...	...

Ledger n	
Bitcoin 1	Adam
Bitcoin 2	Adam
Bitcoin 3	Craig
...	...



Implications

Implications

Price Volatility

- Degree in variation of trading price series over time
- Bitcoin prices fluctuate a lot!
- Lots of speculation
 - Many do not understand the technology
 - Young currency
- Cannot make instantaneous trades like with other currencies
 - Each transaction must be added to the Blockchain
 - Takes about 10 minutes

Implications

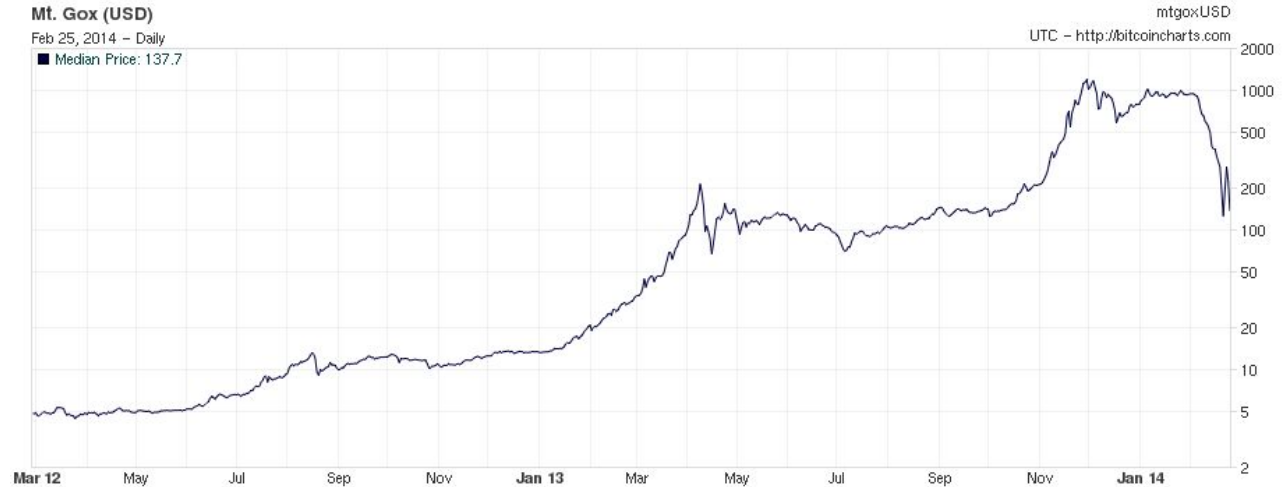
Bank Runs

- Mt. Gox was a Bitcoin exchange based in Tokyo
 - Handled Bitcoin for people
 - Handled 70% of Bitcoin transactions
- Mt. Gox was mismanaged
 - Nearly 450 million USD in Bitcoin disappeared
 - The firm closed their exchange
 - Filed for bankruptcy
- Bitcoin prices plummeted in the aftermath

Implications

Bubbles

- Intrinsic value differs from actual value
- Value of the currency plummeted after Mt. Gox



Implications

Disintermediation

- Bitcoin is decentralized
- Why is this useful?
 - Say I don't trust centralized institutions' currency
 - Bitcoin is an alternative to currencies with greater price volatility
 - Say institutions will not agree to process my transactions
 - Send money to those living under oppressive regimes
 - Crime

Implications

Disintermediation

- Bitcoin isn't necessarily decentralized
 - Anyone who controls 51% of the network can manipulate the ledger
- Why would 51% of the network collaborate?
 - Mining pools reduce pay-out variance
 - People prefer a steady stream of pay-outs for mining
 - Pay-outs in mining are random
- GHash.IO
 - They are a mining pool
 - They controlled 51% of the network at one point
 - They agreed to limit themselves to 39.99% of the network a given time
 - Bitcoin loses value if the control the majority of the network

Questions?