ECE560
Computer and Information Security

Fall 2020

Cryptocurrencies: the Short Version

Tyler Bletsch

Duke University

Structure of this talk based on
[“But how does bitcoin actually work?” by 3Blue1Brown on YouTube]

Cryptocurrency: Origins

- **Regular currency**: Money managed by a central authority. E.g., created by government, non-cash spending tracked by banks.
  - Want to send some money? Record a row into a database. Easy.

But wait! I want a form of money with <u>no central authority</u>!

Also, I want to waste as much electricity as possible,
and I don’t mind if I enable tons of crime.

- Satoshi Nakamoto, probably

Inventing BitCoin

- **BitCoin**: First cryptocurrency, invented by “Satoshi Nakamoto” (pseudonym, identity unknown) in 2008
  - Key innovation: solves the double-spend problem
- Many follow-on cryptocurrencies that make different design decisions
- Key properties in common:
  - **Ledger-based**: The transaction history *is* the currency
  - **Digital signatures on transactions**: Establish identity
  - **Peer-to-peer network:** Decentralizes it
  - **Proof-of-work system**: Miners accept transactions and turn them into blocks in exchange for bonus currency
  - **Block chain**: Prevent double-spend in the long term

Based on “But how does bitcoin actually work?” by 3Blue1Brown on YouTube

Ledger-based with digital signatures

- A ledger is a list of transactions, e.g. "Alice pays Bob $20, Charlie pays Denise $35, etc."
- Anyone can append lines, except:
  - Spender must author the transaction
  - Spender can't spend more than they have
  - Transaction must have a **digital signature** from spender
- Others will verify these properties (covered soon)

Based on "But how does bitcoin actually work?" by 3Blue1Brown on YouTube

Peer-to-peer network

- **Peer-to-peer network**: A network with no clear client/server relationship; all participants are **peers** and can talk to one another
  - Some complexity in finding fellow peers with no central authority to organize, but this is solvable
- Don't want a central authority to own the ledger, so **everyone keeps their own copy of the ledger.**
- Have to **broadcast** transactions to peer network, get them to record it into their ledgers

- Big problem: How to get rest of the world to agree on the same sequence of transactions? This is what BitCoin solved.

Based on "But how does bitcoin actually work?" by 3Blue1Brown on YouTube

Proof-of-work system

- Each client trusts whatever version of the ledger has the most computational work put into it.
  - Goal: Make it computationally infeasible for fraudulent transactions to survive
- Method:
  - Gather many transactions that are being broadcast into a **block**
  - Find a piece of data that, when appended to the block, causes the hash of that data to be ***special*** (e.g., to start with a N zero-bits)
    - Have to try 2^N tries on average to find one! Also, N is configurable.
  - Others can verify this is true quickly; this is a **proof of work**
    - Others also verify all signatures and that nobody overspent

Based on “But how does bitcoin actually work?” by 3Blue1Brown on YouTube

Block chain

- For those **blocks** from before, each must also contain the hash of the previous block
  - This puts them into an order, or *chain* of blocks: the **block chain**
  - Can't change earlier transaction without re-computing *all* the subsequent proofs of work
- Peers trust the *longest* chain
  - Breaks ties, ensures that network trends toward consensus
- Thanks to nodes doing *tons* of computation, 99.999999% of which is wasted, the network arrives at consensus on a single view of the ledger or **block chain**

Based on "But how does bitcoin actually work?" by 3Blue1Brown on YouTube

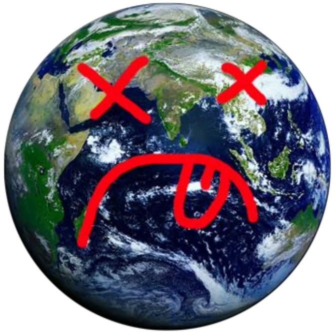
Motivating the waste: Mining

- Wait, why would someone bother doing hours of computation just to validate other peoples' transactions?
  - **We bribe them**: whatever node successfully gets its proof of work accepted is awarded a free transaction that *creates* some Bitcoin for them
  - This is where Bitcoins come from, and it's why they call it "mining" (could really be called "validating other peoples' spending for cash")
  - Miners also earn transaction fees too: **bribes** to include one transaction in an attempt versus another
    - If you try to spend Bitcoin but include too little of a bribe, no miners will include it and the spend will never happen. But it's probabilistic, so you just see it "waiting to go through" for a long time before giving up.
- **Sliding difficulty**: BitCoin protocol sets the difficulty of the proof of work (number of zeroes at the front of the hash) so the average time is ~10 minutes (no matter how many people are mining)
  - Exponentially increasing computation → exponentially increasing cost

Based on "But how does bitcoin actually work?" by 3Blue1Brown on YouTube

Why I hate Bitcoin and think it harms the world: #1. WASTE

- To record a transaction in a traditional system, a database might use 10ms of computation on a 500 W server: 5 J of energy/transaction
- BitCoin: does 4.6 transactions per second (src), uses ~7 GW of power worldwide (src):
  (1/4.6) * 7 GW = 1.5 **G**J of energy/transaction
- The energy use per transaction of BitCoin is
  300 MILLION TIMES WORSE
  - I literally can't think of anything less efficient than this on earth.
- 0.21% of all electricity generated by our species goes into this!
  ¯\_(ツ)_/¯



Why I hate Bitcoin and think it harms the world:
#2. CRIME

- BitCoin is the single reason **ransomware** exists
  - Before, there was safe no way for criminals to charge “customers” (victims)
  - Now, cryptocurrency allows anonymous payments in an automated way
  - Greatly increased motivation of criminal black-hat hackers – new path to revenue!
- Cryptocurrency gives rise to **electronic black markets**
  - Want to charge for your botnet, attack services, child pornography, assassination, fake credentials, or cocaine? BitCoin is for you!
- **Forensic accounting** (tracking money) used to be a top method of law enforcement against cyber criminals. Now it’s not. ¯_(ツ)_/¯

Why I hate Bitcoin and think it harms the world:
#3. WALLET SECURITY

- Your private key ("wallet.dat") ***is*** the money,
  if it's stolen, nobody can help you.
  - In traditional currency

    Victim: "My card was stolen, freeze it immediately and reverse the charges!"
    Bank: "Of course, and we'll cover the losses."
  - In cryptocurrency

    Victim: "Hello, computer programs! My wallet.dat was stolen!"
    Nobody: ¯_(ツ)_/¯
  - $1.1 BILLION in cryptocurrency was stolen in 2018 (src).
  - Not just individuals, **currency exchanges** are frequent targets, as "remote shell" now equals "direct access to millions of dollars"
- Also, if you lose that file, you lose the money irrevocably
  - In fact, 20% of all BitCoin mined is eventually lost forever (src)

Conclusion

- Cryptocurrency:
  - Interesting application of cryptography to solve a hard problem:
    a decentralized tamper-resistant public ledger system
  - Downsides: garbage efficiency, garbage security, incentivizes crimes
- Blockchain in general:
  - A lot of interest in blockchain for other purposes (much of it stupid)
  - Do you need a globally writable public ledger where nobody is trusted, and you’re willing to have absolute garbage time and energy efficiency to do so?

    Then check out ~~block chain~~ revising your requirements to be less insane!