# Bitcoin – part 2

CS 161 Fall 2021 - Lecture 17

# Announcements

- Started recording
- Midterm Thursday, Oct 7, 7-9pm
  - All logistics are on the website
  - Piazza @479 for logistics questions

# Recall: Two components

1. **Ledger/blockchain:**
    1. publicly-visible,
    2. append-only, and
    3. immutable,

    Log

        via hash chain and consensus with proof of work

2. **Cryptographic transactions**

        via digital signatures

# Recall: cryptographic transaction

- Identity is PK
  - Being able to use SK is proof of owning the identity

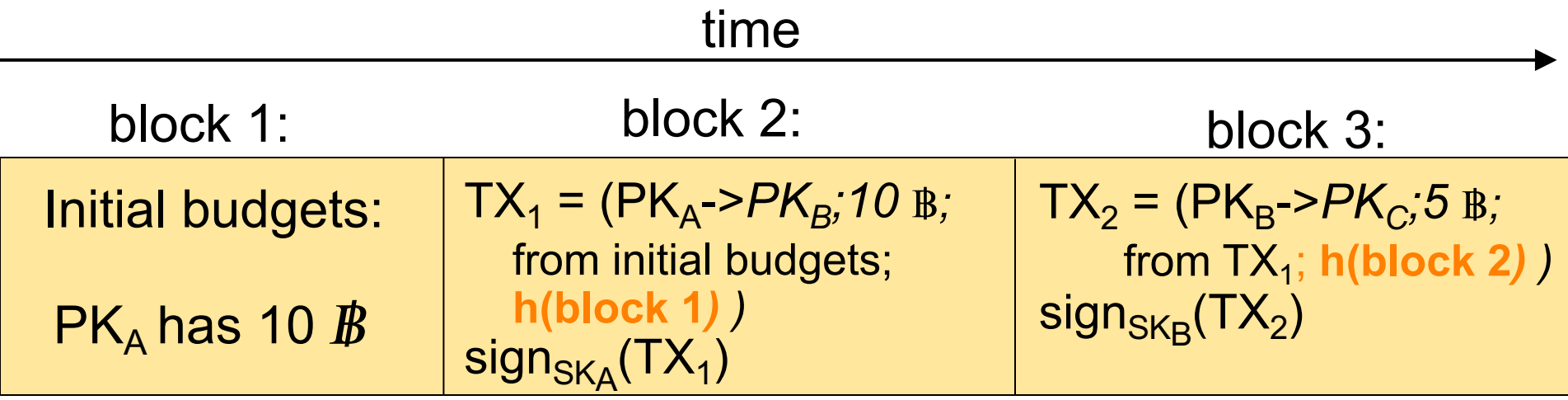
$TX = (PK_{sender}\text{->}PK_{receiver}; X\ ฿;\quad PK_{sender}\text{->}PK_{sender}; R\ ฿;$
list of transactions L where money came from)

time

| Initial budgets:<br><br>$PK_A$ has 10 ฿ | $TX_1 = (PK_A\text{->}PK_B; 10\ ฿;$ from initial budgets)<br>$sign_{SK_A}(TX_1)$ | $TX_2 = (PK_B\text{->}PK_C; 5\ ฿;$<br>$PK_B\text{->}PK_B; 5\ ฿;$<br>from $TX_1$)<br>$sign_{SK_B}(TX_2)$ |
|---|---|---|

# Blockchain

- Chain transactions using their hashes => hashchain
- Each transaction contains hash of previous transaction **(which contains the hash of its own previous transaction, and so on)**
- Recall that a cryptographic hash is collision resistant




block i refers to the entire block (transaction description and signature), so the hash is over all of this

# Consensus

- Every participant stores a copy of the blockchain
- Miners mine blocks by solving proof of work
  - Find random number s.t. Hash(block || random_number) = 000…0000453a48b244

- When someone wants to create a new transaction, they broadcast the transaction to all miners
- Everyone (miners, other participants) always prefer the longest correct chain.
- If majority of compute power is in the hands of honest miners, longest correct chain is with them too.

# “Longest chain” wins

- Problem: What if two different parts of network have different hash chains?

- Solution: Whichever is “longer” wins; the other is discarded

# How can we convince people to mine?

- A: Give a reward to anyone who successfully appends – they receive a free coin
  - Essentially they may include a transaction from no one to their PK having a coin

- Q: What happens to a miner's reward if his block was removed because an alternate longer chain appears?
- A: The miner lost their reward. Only the transactions and rewards on the longest chain "exist".

# Proof of work can be adapted

- Mining frequency is ~10 mins
- If it takes too long to mine on average, make the proof of work easier (less zeros), else make it harder (more zeros)
- Q: what is the economic insight?
- A: if mining is rare, it means few machines in the network, give more incentives to join the network

# Let’s chew on consensus

- Q: What happens if Miner A and Miner B at the same time solve a proof of work and append two different blocks thus forking the network?
- A: The next miner that appends onto one of these chains, invalidates the other chain. Longest chain wins.

- Q: If a miner included your transaction in the latest block created, are you guaranteed that your transaction is forever in the blockchain?
- A: No, there could have been another miner appending a different block at the same time and that chain might be winning. So wait for a few blocks, e.g. 6 until your transaction is committed with high probability, though you can never be sure.

# Let’s chew on consensus

- Q: What happens if a miner who just mined a block refuses to include my transaction?
- A: Hopefully the next miner will not refuse this. Each transaction also includes a fee which goes to the miner, so a miner would want to include as many transactions as possible

# Watch the blockchain live

- https://blockchain.info/

# Bitcoin

- Public, distributed, peer-to-peer, hash-chained audit log of all transactions (“block chain”).
- Mining: Each entry in block chain must come with a proof of work (its hash value starts with *N* zeros). Thus, appending takes computation.
- Lottery: First to successfully append to block chain gets a small reward (if append is accepted by others). This creates new money. Each block contains a list of transactions, and identity of miner (who receives the reward).
- Consensus: If there are multiple versions of the block chain, longest one wins.

# So far …
# unbiased Bitcoin technical design

# Cryptocurrencies have supporters and opposers

# Supporters say…

- No need to trust or depend on banks or the government
- “Digital gold” 
- User in control of their funds despite government policies or banks restrictions/crashes
- Transactions are pseudonymous
- Peer to peer, do not need approval of other entity
- No banking fees
- Low transaction fees for international payments
- Transactions are irreversible
- Anybody can partake, even people without bank accounts

# Critics say…

- It brings waste (e.g., proof of work, many large copies of blockchain)
- Not as decentralized as we wished
- Not scalable
- Market fluctuations
- Not really anonymous
- Irreversible
- No security in case of loss
- Helps criminals, ransomware

# What I think about it

- It has pros and cons
- I think they have brought about some very interesting and creative techniques in cryptographic systems, and stirred much innovation beyond Bitcoin:
  - smart contracts
  - consensus protocols
  - zero knowledge proofs and ledgers
  - blockchains and ledgers for medical and financial use cases
  - ledgers like Certificate Transparency solving decade old problem

# Much innovation after Bitcoin

- I think the Bitcoin protocol is a strike of genius, because of the very creative way of combining different techniques, even if not perfect
- Lots of active development and ideas:
  - Proof of stake, Federated Byzantine agreement, Random committee selection (Algorand), …
  - ZK rollups for scalability
  - More progress needs to be made to solve some problems, but progress has been steady
- They also increased the public's awareness towards the power of cryptography

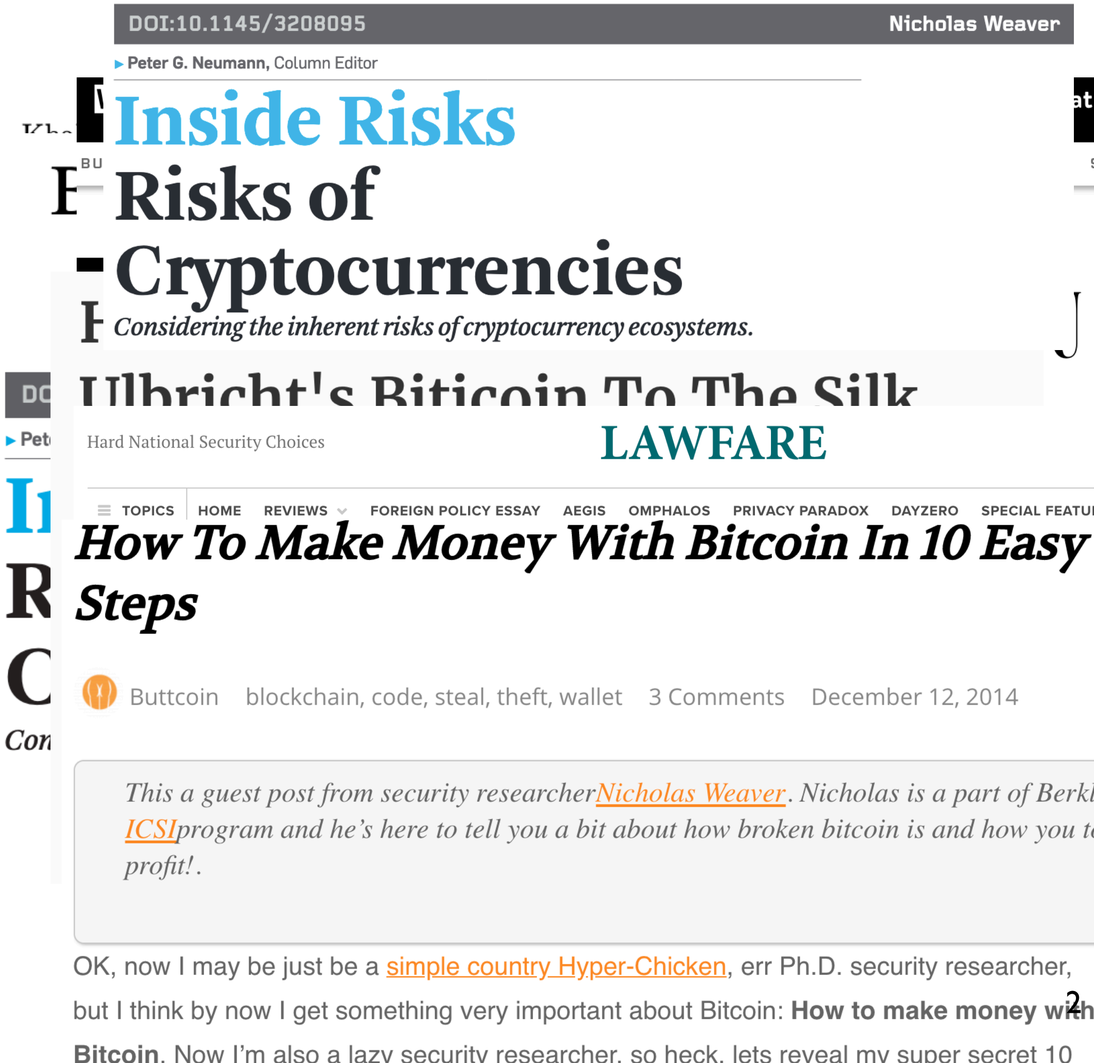
# Blockchains and Cryptocurrencies: DIE IN A FIRE




# Why Is Cryptocurrency A Trash Fire?



- Disclaimer: Opinions are Nick's alone
  - Mining this space for comedy godl [sic], academic papers and general interest articles since 2013
- They can't work for legal payments
  - But do facilitate a multi-billion-dollar criminal ecology
- There is a ***ton*** of trust and central authorities in the system, their presence is just ignored
  - It is 9 ***orders of magnitude*** less efficient than distributed systems which ***articulate*** trust
- "Smart" contracts & "Decentralized" Apps/Finance aren't
- The entire space is a deeply negative sum natural Ponzi scheme
  - With a bunch of Live Action Roll Players (LARPers) replaying half a millennia of various financial failures



DOI:10.1145/3208095 Nicholas Weaver

Peter G. Neumann, Column Editor

Inside Risks

Risks of Cryptocurrencies

*Considering the inherent risks of cryptocurrency ecosystems.*

Ulbricht's Bitcoin To The Silk

Hard National Security Choices

LAWFARE

TOPICS HOME REVIEWS FOREIGN POLICY ESSAY AEGIS OMPHALOS PRIVACY PARADOX DAYZERO SPECIAL FEATU

***How To Make Money With Bitcoin In 10 Easy Steps***

Buttcoin blockchain, code, steal, theft, wallet 3 Comments December 12, 2014

*This a guest post from security researcherNicholas Weaver. Nicholas is a part of Berk ICSIprogram and he's here to tell you a bit about how broken bitcoin is and how you t profit!.*

OK, now I may be just be a simple country Hyper-Chicken, err Ph.D. security researcher, but I think by now I get something very important about Bitcoin: **How to make money with Bitcoin**. Now I'm also a lazy security researcher, so heck, lets reveal my super secret 10

# Irreversibility & Incompatibility

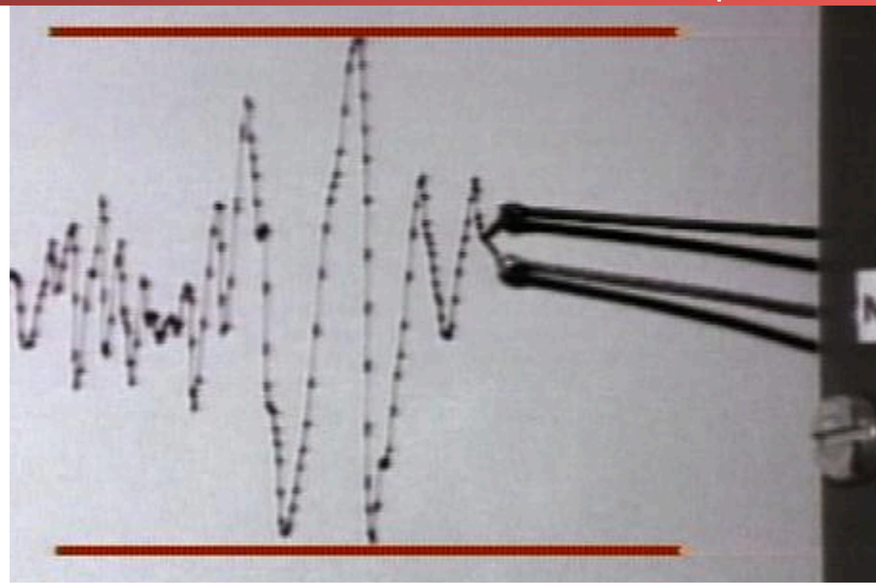


- Remember the premise:
  Alice sends 100 Dunning/Kreuggerands to Bob with ***no intermediaries*** that can block or reverse the transaction
- Modern finance:
  Everything electronic ***must be reversible*** for a limited period of time
  - Enables fraud ***mitigation***: detect & respond, not just prevent fraud
- Means buying cryptocurrencies is expensive:
  - Ether the seller is giving credit
  - Or the seller must accept cash
  - Or the seller needs to wait
- And they are hard to store as well
  - If someone gets your private key...

# So They Can't Work For Legal Payments!



- Any volatile cryptocurrency transaction for real-world payments requires two currency conversion steps
  - It is the only way to remove the volatility risk
    - Which is why companies selling stuff aren't actually using Bitcoin, but a service that turns BTC into Actual Money™
  - But if you believe in the cryptocurrency, you must hodl!
- Result is that the promised financial applications can never apply in volatile currencies like Bitcoin
  - Really Bitcoin et al are only appropriate for buying drugs, paying ransoms, hiring fake hitmen, money laundering...



# And "Stablecoins" are no solution...



- Stablecoin: You have a trusted entity that takes dollars and issues cryptodollars
  - And will go the other way
  - This is called a ***bank*** and these are called ***banknotes***!
- Pick one (or more) of three options
  - Be Visa or a regulated bank
    - No more anonymity, no more avoiding the laws
  - Be a "Wildcat Bank" from the 1800s
    - Print banknotes that aren't actually backed:
      Tether appears to prints new Tethers, loan them to associated entities which then buy up cryptocurrencies driving up the prices
  - Be "Liberty Reserve"
    - Avoid the laws...
      And meet up with the FAFO Alligator


**Department of Justice**

Office of Public Affairs

FOR IMMEDIATE RELEASE Friday, May 6

**Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions Dollars**

Arthur Budovsky, 42, was sentenced today in the Southern District of New York to 20 years imprisonment for running a massive money laundering enterprise through his company Liberty Reserve S.A. ("Liberty Reserve"), a virtual currency used by cybercriminals around the world to launder the proceeds of their illegal activity.

# Bitcoin's Crime Against Nick:
# It Made Him BELIEVE In Money Laundering Laws



- There are lots of laws imposed on banks & money transmitters
  - AML: Anti-Money Laundering
  - KYC: Know Your Customer
- Cryptocurrency is ***designed*** to bypass all of this
  - "Censorship resistance"
- This has enabled crime both minor (online drug markets) and major (ransomware)
  - Ransomware: Break into a business, encrypt the data with a public key scheme and demand M$ to release the session keys to get the data back, a multi-billion-dollar a year mostly Russian industry
  - Regularly disrupts pipelines, hospitals, and many other businesses all the time
- Ransomware is entirely dependent on cryptocurrency
  - Banks would refuse to process ransom payments
  - Cash is heavy and would require picking up in person

# Mining, Sibyls & The Red Queen's Race

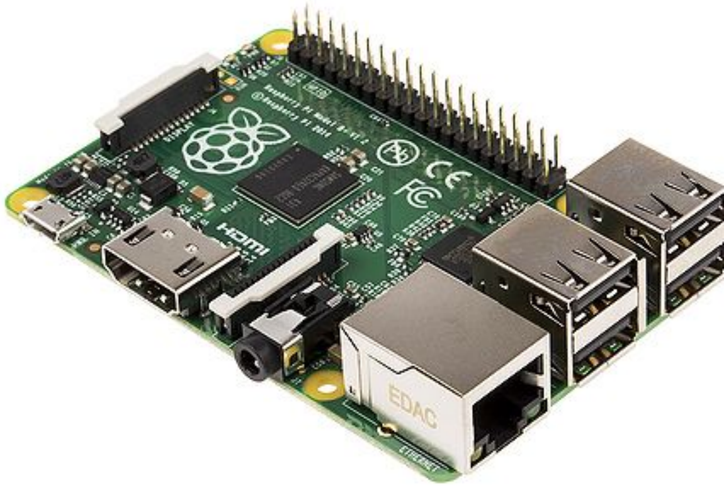


- Proof of Work mining creates a "Red Queen's Race"
  - As long as there is more profit to be had, more mining occurs
  - Net result is that, in steady state, all profits end up paying for electricity and mining rigs
  - Currently Bitcoin is ~= Romania in power consumption and Ethereum is ~= Bangladesh
- And really this is about solving the "sibyl problem"
  - Someone creates a ton of fake identities:
    Proof of work is really proof of wasting energy as a way of preventing this

# Security is Economics: PoW "Security" is Criminally Inefficient



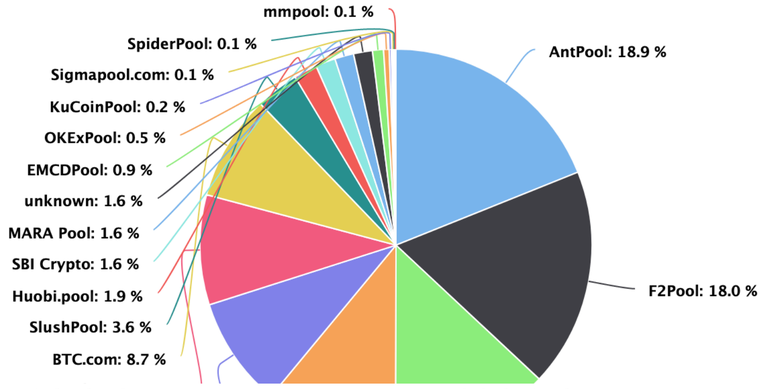
- Proof of work is provably wasteful
  - It is proof of burning $X/hr on a system-wide basis
- The security equation
  - An attacker can earn $Y in an attack taking time T
  - PoW is secure if-and-only-if Y < XT
  - But an attacker only needs to attack for time T, defenders need to spend 24/7/365!
- This also affects the real-world "wait" for security
  - If your worry is attacks and you receive a value Y...
    You haven't really received it until Y/X time passes!
- So "articulated trust" is vastly cheaper
  - Take 10 trustworthy entities, each one has a Raspberry Pi that validates and signs transactions. In the end, 6 need to be honest (majority voting consensus)
  - This requires 100W of power and $500 worth of computers:
    9 ***orders of magnitude*** less power
  - But identified entities would need to respect KYC/AML regulations
    and couldn't justify a $1T "market capitalization" for a system like that!



# And There is a Ton of Trust in the "Trustless" Systems



- You have to trust at least a majority of the miners
  - So that 10x Raspberry Pi system is more meaningfully distributed in terms of trust!
- You have to trust the developers
  - They can and ***have*** reversed transactions even when proclaiming "Code is law!"
- You have to trust the libraries the developers use
  - Libraries can and ***have*** been corrupted to steal cryptocurrencies
- You have to trust the code things depend on is all ***bug free!***
  - Because bugs can otherwise result in loss or theft




*"The development community is proposing a soft fork, (with NO ROLLBACK; no transactions or blocks will be "reversed") which will make any transactions that make any calls/callcodes/delegatecalls that execute code with code hash (ie. The DAO and children) lead to the transaction (not just the call, the transaction) being invalid, preventing the Ether from being withdrawn by the attacker past the 27-day window. This will later be followed up by a hard fork which will give token holders the ability to recover their Ether."*

kaspersky daily

supply chain

## A bad link in the cryptochain

A supply-chain attack against Copay cryptowallets through an open-source library enables bitcoin theft.

{* SECURITY *}

## Android bug batters Bitcoin wallets

Old flaw, new problem

Richard Chirgwin

# "Smart" Contracts & "Decentralized" Finance



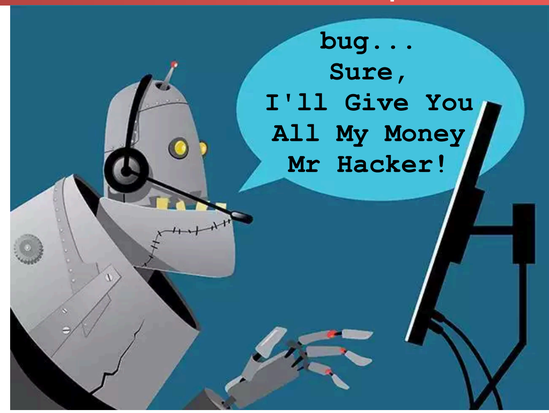
- Real contracts are written in a formal-ish language called "legalese"
  - Sorta looks like English but not really
  - Standard contracts are cheap-to-free
  - Bespoke contracts are horribly expensive to create
- Remarkably forgiving formal-ish language:
  - There is a robust exception handling mechanism called "lawyers", "arbiters", and "courts"
- Hey, "Code is Law"!
  - Lets change the language to something even uglier, remove the exception handling mechanism, and call it good!
  - Programs are deterministic:
    Every miner may run the program but will always get the same result

Contract Source Co

```
104     /*=======
105     =            EV
106     ============================*/
107     event onTokenPurchase(
108         address indexed customerAddress,
109         uint256 incomingEthereum,
110         uint256 tokensMinted,
111         address indexed referredBy
112     );
113
114     event onTokenSell(
115         address indexed customerAddress,
116         uint256 tokensBurned,
117         uint256 ethereumEarned
118     );
119
120     event onReinvestment(
121         address indexed customerAddress,
122         uint256 ethereumReinvested,
123         uint256 tokensMinted
124     );
125
126     event onWithdraw(
127         address indexed customerAddress,
128         uint256 ethereumWithdrawn
```

# Reality:
# (Low Performance) Finance Bots



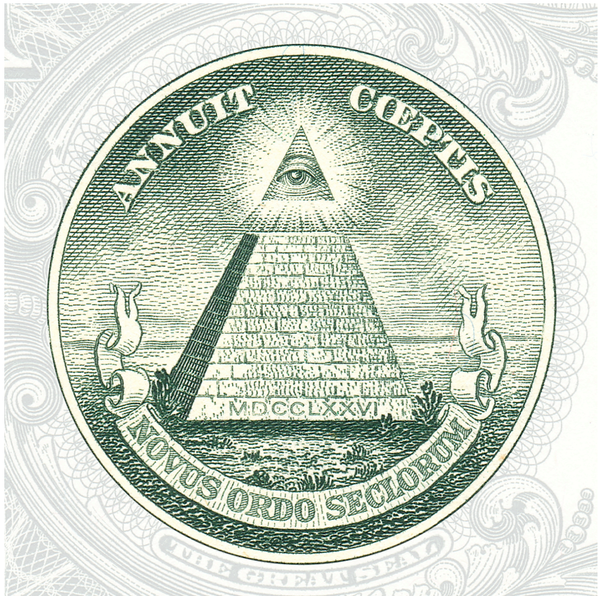



- Small programs that operate on money
  - "Piñatas for Blackhats to whack until the money rains out"
    -David Gerard
    - Record exploits have reached into hundreds of millions of $ of value!
- The real world has used finance bots for decades
  - But without public interaction (for exploitation) and on reversible fabrics (for bug mitigation)
- And the performance is dismal:
  - The Ethereum network's ***productive*** compute is ~1/10,000 of a RPi 4!
- So why "DeFi"?
  - "Can't sue me Bro, it is the decentralized program running the Ponzi scheme or creating the unregulated exchange in violation of every securities law!"
    - Please ignore that if the developers can fix bugs after release they are the central authority responsible for the particular code

# Finance is ***all*** zero sum at best



- Every dollar "made" in cryptocurrency came from someone else
  - There is no dividends or interest flowing in unlike the stock or bond market
  - The ledger's utility value is effectively $0:
    It is just a cryptographic timestamp service with a hash chain
    - Service that takes H(M), returns Sign(H(M),T,H(Last Signed))
      Ideas that have existed for 20+ years
- There is one other financial instrument like this: A Ponzi scheme
  - "Profits" from early investors is payment from the later investors
  - Note that formal Ponzi schemes are a criminal fraud!
    And lots of such explicit schemes in cryptocurrency-land



# The Rest Is LARPing a Speedrun of 500 years of bad economics...



- "Gold Standard/Hard Money" types
- Almost every cryptocurrency exchange is full of frauds banned in the 1930s
- Ponzi schemes without postal reply coupons, including explicit ponzies as "Smart Contracts"
- Every tradable ICO is really an unregulated security just like the plagues in the South Sea Bubble of 1720 usually as a "Smart Contract"
- Replicated rare tulips with rare cats on the Ethereum Blockchain as a "Smart Contract"! Time to party like it is 1637!


# What About Non-Currency Blockchain Applications?



- Put A Bird Blockchain On It!
- "Private" or "Permissioned" Blockchain
  - Simply a cryptographically signed hashchain:
    Techniques known for >20 years!
  - The only value gained is you say "Blockchain" and idiots respond with "Take My Money!"
- "Public" Blockchains are grossly inefficient and can't actually deliver on what they promise
- And those proposing "blockchain" don't actually understand the problem space!
  - Solve (Voting, electronic medical records, food security, name your hard problem) by putting {what data exactly? How? What formats? What honesty? What enforcement?} in an append-only data structure
- Nick's Iron Law of Blockchain:
  "Anyone who says ***Blockchain can solve X*** doesn't understand X and can be safely ignored"

# Solution?



- Actually ***Enforce the LAWS!***
  - Cryptocurrency's only "value" is evading regulations...
    So don't let them!
- Every ICO is an unlicensed security: the ***Howey*** test
  - "An investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party, it being immaterial whether the shares in the enterprise are evidenced by formal certificates or by nominal interests in the physical assets employed in the enterprise."
- Lots of money transmitters who aren't acting like it
  - The cryptocurrency miners ***are*** money transmitters, they ***can and have censored transactions!***
- Lots evading consumer protection regulations
  - Your bank account gets hacked?  You get made whole
  - Your coinbase account gets hacked?  Sorry for your loss!
- Lots of "Decentralized in Name Only" DeFi systems
- And lots and lots and lots of outright criminality

# So Where Does This Leave Us?