Crypto 6: Voting and Blockchains

-Lea Kissner

Administrivia!

- Reminder:
  - Zoom chat for conversation
  - Zoom Q&A for Questions & Answers

Voting:

- Voting is one of the hardest ***system*** security problems out there
  - And often the best solutions are to ***limit*** the impact of computers
- Quantifying the problem:
  - Every person ***must*** only be able to vote one time
  - Every person ***must not*** be able to prove who they voted for
    - Secret ballot/deniability
  - People ***need to have confidence*** that votes are correctly tallied
    - Limits crypto-magic:
      Hard hard hard to explain and hard to engineer for both "You can prove your vote got counted" but can't "Prove what your vote was"
  - Practical fraud limit: ***all*** fraud scenarios which require changing at least ***n*** votes should require O(***n***) effort!

Consists of ***many many*** moving parts

- Voter Registration database
  - A list of all ***eligible*** voters
- The Poll Book
  - A local list of who is eligible to vote here:
    Check off names of people as they vote
- Vote recording system
  - The system you interact with to do the actual voting
- Vote tabulation
  - The system that sums up all the votes

Vote Recording Systems

- A particular focus on Vote recording systems
  - Out of the 2000 "hanging chad" debacle in Florida
- Touchscreen/computer only
  - CLEARLY awful: no way for a voter to verify their vote is recorded: Fraud becomes O(1)!!!!!
  - But no known ***instances*** of widespread computer-based fraud!
    - Only known instances have been poll workers casting a bunch of additional votes:
      Which they could just as easily do with paper ballots ("Stuffing the ballot box")
- Touchscreen with printout
  - Ballot Marking devices:
    You ***must*** ensure that the output matches your vote
    Output ***must*** be human readable
- Good old paper
  - What most of us like

Electronic Poll Books...

- ***These*** will be the problem this time around
  - Many states have already replaced DRE machines with systems that produce a paper trail
- Advantages:
  - No longer need to tell everyone to vote at a particular location:
    Instead go to any of several locations
- Disadvantages:
  - Poll workers & voters often find them a lot slower/harder to use
  - Potentially vulnerable to hacking as a disruption tactic
- Already some court cases:
  - Georgia now required to have paper back-up on the day-of voting

Fake "Voter Fraud" 1: Photo Identification requirements

- The Republicans in the US uses ***false*** cries of voter fraud: Need for "Photo ID" for in-person voting
- Voter impersonation fraud is ***very very very rare***
  - It is an expensive, risky, and ineffective O(***n***) with a very high constant factor
  - Anyone who talks about hordes of fake voters casting fraudulent in-person ballots is either delusional or deliberately lying
- Rather this is part of a voter suppression effort by Republicans
  - Getting an ID is not a trivial task: Made worse with the Real-ID crap
  - Poor are far less likely to have a photo ID... and far more likely to vote D

Fake "Voter Fraud" 2: Mail-in ballots

- Mail-in ballots are weaker to vote buying and coercion
  - Because it is much easier to prove you are "voting right" when marking your ballot
  - But this is still an O(***n***) fraud and still an expensive fraud
- They receive similar (or even heightened) scrutiny against other fraud
  - Exterior envelope contains the voter name and signature
  - Cases of rogue "harvesters" have changed perhaps a few hundred votes
- Claims of "widespread fraud" are simply false
  - Instead intended for voter suppression:
    Either get people not to vote OR try to get them thrown out in the courts
  - Oh, and to placate the ego of the Orange One should he lose

Our Ugly November

- The first week in November may be very ugly
  - Perhaps day-of security attacks: targeting the poll books & registration databases
  - Post-election fights over vote counting seem inevitable
    - If you want nightmare fuel, read the Barton Gellman piece in the Atlantic: https://www.theatlantic.com/magazine/archive/2020/11/what-if-trump-refuses-concede/616424/
  - Perhaps even a low grade insurgency:
    Trump Jr has already used "we need all able bodied volunteer" type rhetoric and there are already a lot of ~~militia groups~~ groups of armed thugs springing up around the US
- I will be here to support everyone...
  - ***No projects*** will be due that week
- But at that point ***we are simply passengers***
- So ***you*** need to vote ***AS SOON AS YOU POSSIBLY CAN***

Voting Step 1: Validate Voter Registration

- If you aren't yet registered but are eligible... ***REGISTER***!
- If you are registered, ***check!***
  - There are online sites for each state that allow you to check
- Decide how you are going to vote:
  - Absentee/by mail
    - Everyone in CA should get a ballot automatically in the mail
  - In person

Vote Step 2:
VOTE IN PERSON

- If you are voting in person...
- Check for availability of ***early voting***
  - Generally more centralized/fewer locations...
  - But it allows you to vote now rather than waiting for election day
  - And get out and VOTE!
- If no early voting and voting in person...
  - Be prepared to wait in line:
    Especially if you are in a more Democratic area of a Republican-controlled states
- Follow instructions carefully on marking the ballot
  - Or if your voting uses some touchscreen device, ***verify*** that the output matches if possible
  - But even if you have touchscreen-only, ***vote anyway!***

Vote Step 2: VOTE BY MAIL

- Make sure you have already requested your absentee ballot
  - Rules vary by state
- If the state supports it, track your ballot!
  - California does: https://california.ballottrax.net/voter/
- As soon as you get your ballot
  - ***READ THE INSTRUCTIONS CAREFULLY before filling it out***
  - A lot of states have arcane rules:
    South Carolina: you must have a witness sign the envelope too
    Pennsylvania: your ballot must be in a security envelope that is sealed and then in the outer envelope
- Fill it out and return it ***immediately***
  - If there are drop boxes you can use, use a drop box
  - Otherwise, mail it right away: Again, signs of deliberate voter suppression in disrupting mail service and trying to require delivery on election day (rather than postmark)

Vote Step 3:
Tell your friends to vote!

- If you don't vote, your vote doesn't count
- If your friends don't vote, ***their votes don't count***
- You notice how there is a fair amount of local research needed
  - But once you do it, tell your friends in the area!
- Who knows...
  Requirements for voting in your area may be questions on the midterm!

Why Talk About Cryptocurrencies?!?

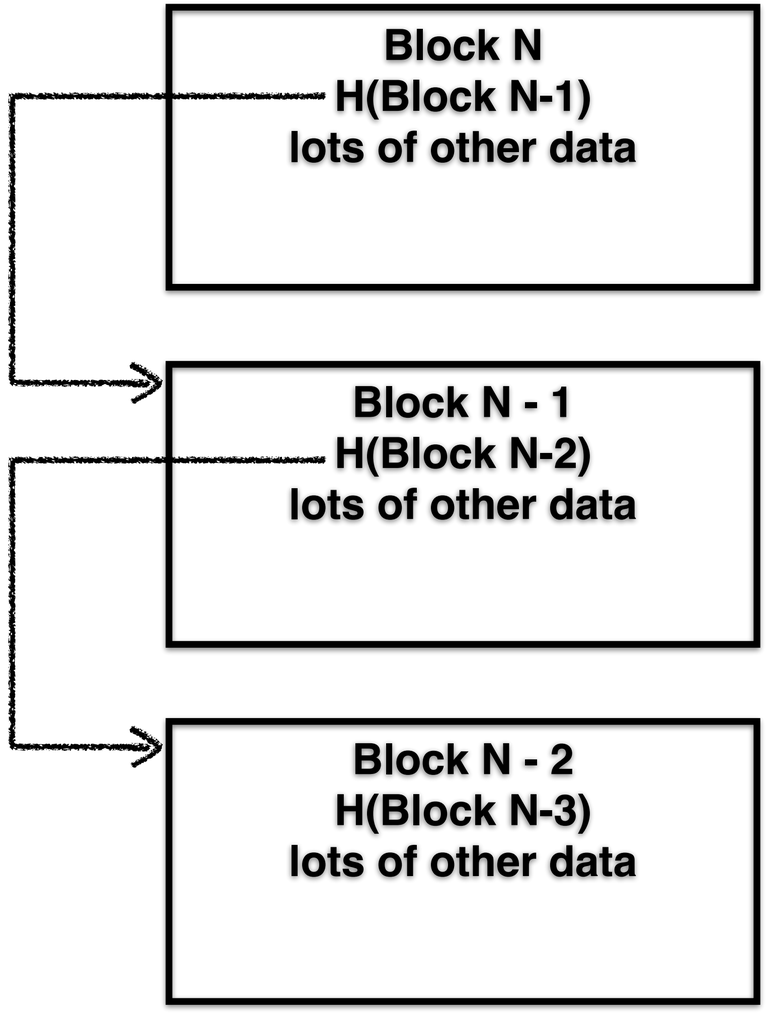
- I am an actual ***expert*** in this area
  - It has been one of my research focuses for the past 5+ years!
- But I want it to die in a fire!
  - There is effectively no value:
    - Private Blockchains are 20+ year old ideas
    - Public Blockchains are grossly inefficient in the name of "decentralization" without actually being decentralized!
      - And don't actually solve any problems other than those required to implement cryptocurrencies!
    - Cryptocurrencies don't work as currency unless you are a criminal!
- Yet it has refused to just go away

~~Linked Lists~~ Blockchains And CryptoCurrencies

- "Blockchain Technology"
  - A fancy word for "Append-Only Data Structure"
    - That causes people's eyes to glaze over and them to throw money at people
  - "Private/Permissioned Blockchain":
    - A setup where only one or a limited number of systems are authorized to append to the log
    - AKA 20 year old, well known techniques
  - "Public/Permissionless Blockchain":
    - Anybody can participate as appenders so there is supposedly no central authority: Difficulty comes in removing "sibyls"
- Cryptocurrencies
  - Things that don't actually work as currencies…

Hash Chains

- If a data structure includes a hash of the previous block of data: This forms a “hash chain”
- So if you have a way of validating the ending block: The inclusion of the previous block’s hash validates all the previous blocks
- This also makes it easy to add blocks to data structures
  - Only need to hash block + hash of previous block, rather than rehash everything:
    How you can efficiently hash an "append only" datastructure
- Now just validate the head (e.g. with signatures) and voila!
  - All a “blockchain” is is a renamed hashchain!
    Linked timestamping services used this structure and were proposed back in 1990!



Merkle Trees

- Lets say you have a lot of elements
  - And you want to add or modify elements
- And you want to make the hash of the set easy to update
- Enter hash trees/merkle trees
  - Elements 0, 1, 2, 3, 4, 5...
  - H(0), H(1), H(2)...
  - H(H(0) + H(1)), H(H(2)+H(3))...
  - The final hash is the root of the top of the tree.
- And so on until you get to the root
  - Allows you to add an element and update lg(n) hashes Rather than having to rehash all the data
  - Patented in 1979!!

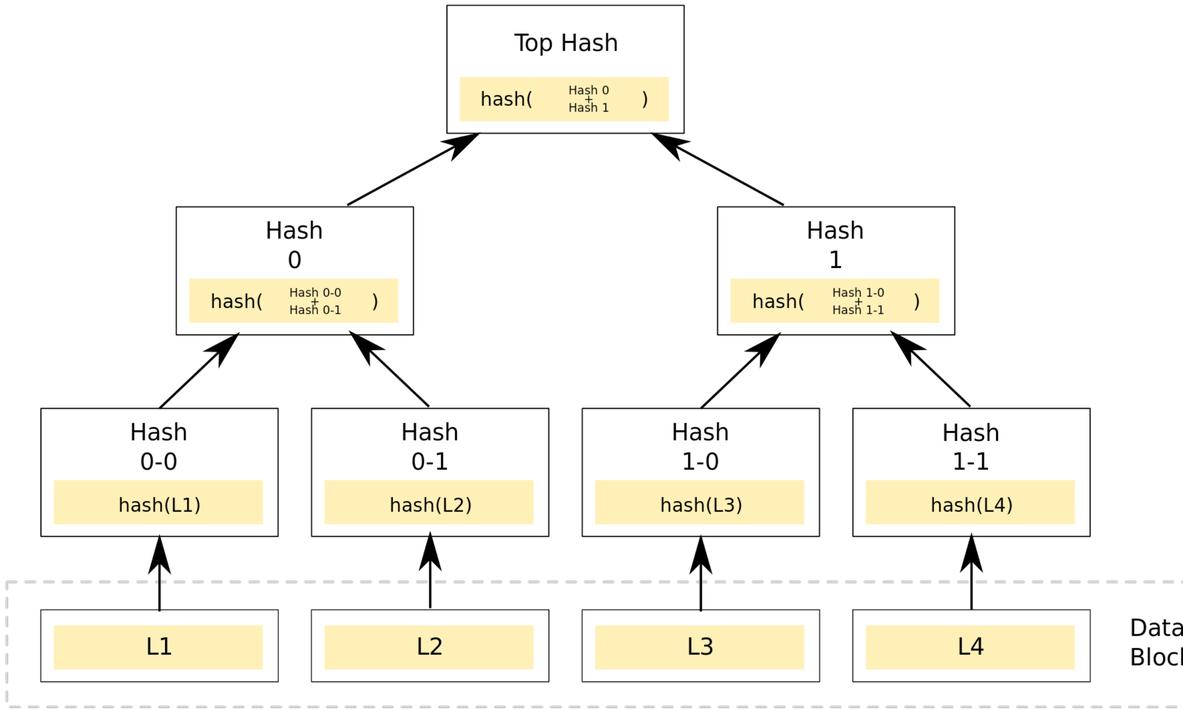


Image Stolen from Wikipedia

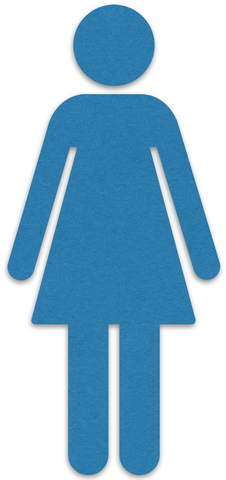
A Trivial Private Blockchain…

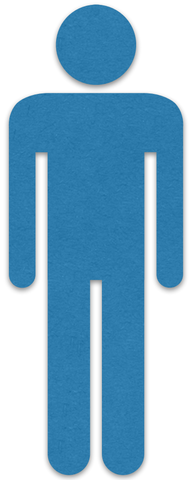
- We have a single server ***s***, with keys K_{pub} and K_{priv}…
  - And a git archive ***g***… (in which we fix git to use SHA-256)
- Whenever we issue a pull request…
  - The server validates that the pull request meets the allowed criteria
  - Accepts the pull request
  - Signs the hash of the head…
- And that is it!
  - Git is an append only data structure, and by signing the new head, we have the server authenticating the ***entire archive!***
- This is why “private” blockchain is ***not*** a revolution!!!
  - Anything that would benefit from an append-only, limited writer database already has one!

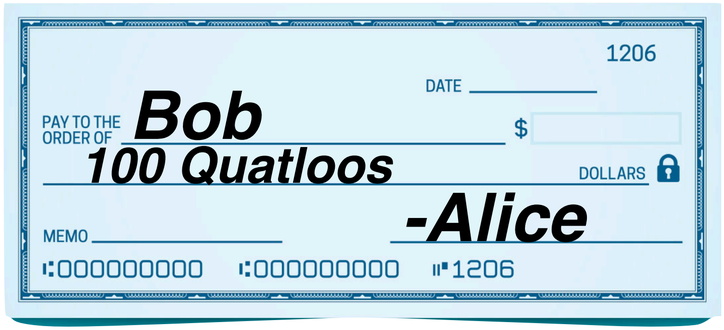
What Is A "Cryptocurrency"?

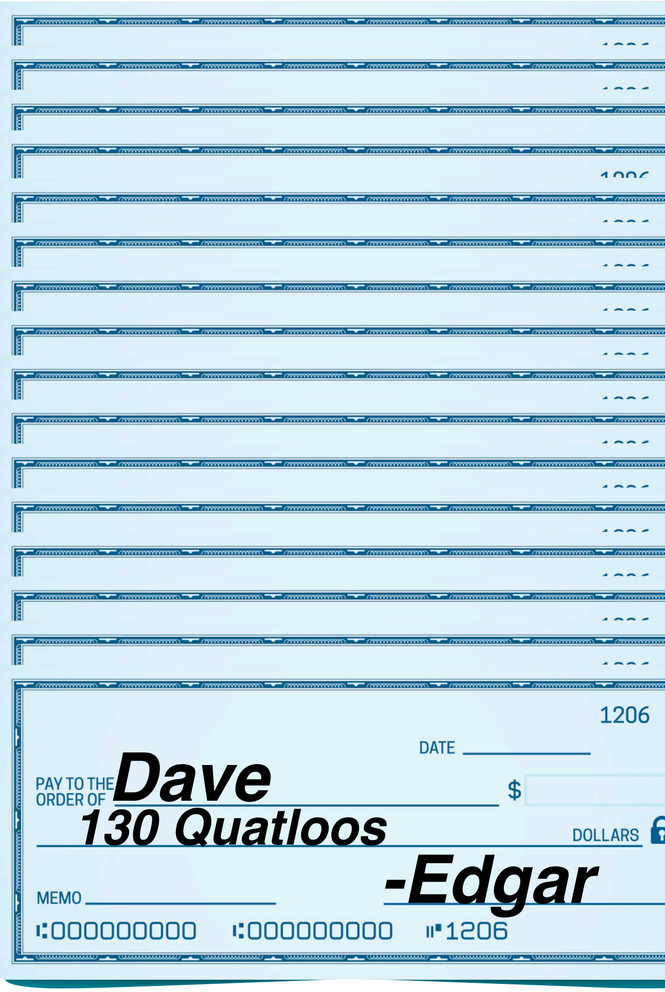
- A cryptocurrency is a tradable cryptographic token
  - The goal is to create irreversible electronic cash with no centralized trust:
    If Alice wants to pay Bob 200 Quatloos to pay off her losing bet on the Green thrall, there should be ***nobody else who can block or reverse this transfer***
- Based on the notion of a public ledger (the "Blockchain")
  - A public shared document that says "Alice has 3021.1141 Quatloos,
    Bob has 21.13710 Quatloos,
    Carol has 1028.8120 Quatloos..."
  - People can ***only*** add items to the ledger ("append-only"), never remove items
- Big Idea: Alice writes and signs a check to Bob saying "I, Alice, Pay Bob 200 Quatloos"
  - This check then gets added to the public ledger so now everyone knows Alice now has 2821.1141 Quatloos and Bob has 221.13710 Quatloos

What Is A "Cryptocurrency"?





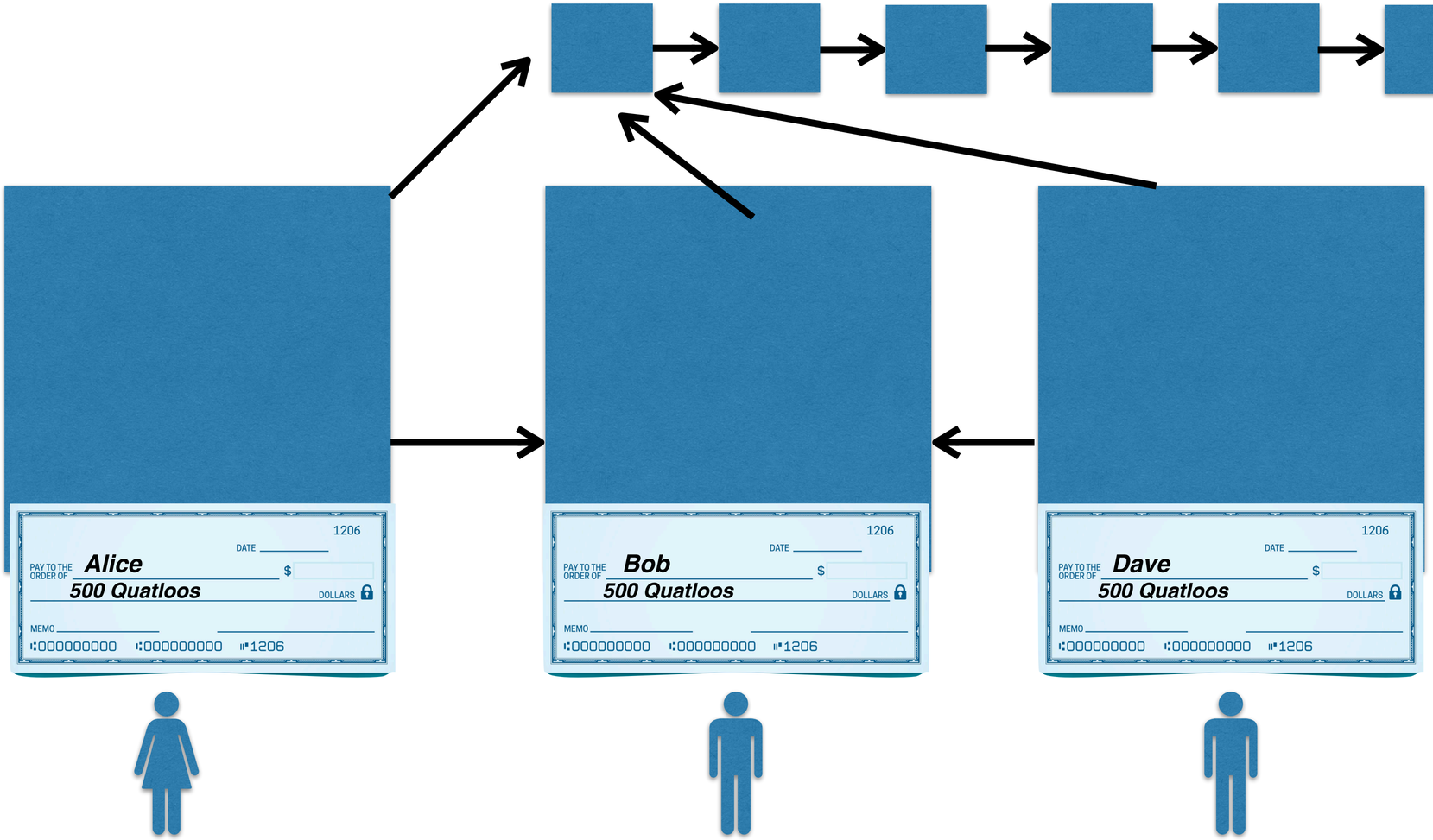




What Is A "Blockchain" (well, "Public" or "Permissionless" Blockchains)

- Everyone involved gathers up copies of the loose checks
  - For each check, validate that there are sufficient funds
  - Bundle all the checks up into a "block" and staple them together, with a pointer to the previous pile
- Everybody now does a lot of useless "work" that may eventually get lucky
  - The one that gets lucky staples this (which is in the form of a check saying "The system pays to ME the reward for success" and the staple that binds everything together) to the block as well, publishes this, and gets the reward
- Now everybody else knows this stapled pile of checks is now verified
  - So everybody starts on a new block, pointing to the previous block and gathers up the new checks that haven't yet been processed
- Result is an ***append only*** data structure

What Is A "Blockchain" (well, "Public" or "Permissionless" Blockchains)



What Is Bitcoin?

- Simply the first widespread development of this idea
  - A "Bitcoin wallet" is simply a collection of cryptographic keys
    - Private key K_{priv}: A secret value stored in the wallet
    - Public key K_{pub}: A public value that anybody is allowed to see, derived from the private key
  - The "Bitcoin Blockchain" is Bitcoin's particular implementation of the shared ledger
- Spending Bitcoin is simply writing a check and broadcasting it:
  - "Pay K_{pub}=1Ross5Np5doy4ajF9iGXzgKaC2Q3Pwwxv the value 0.05212115 Bitcoin...
    And whoever validates this transaction gets 0.0005 Bitcoin"
    - Signed 1FuckBTCqwBQexxs9jiuWTiZeoKfSo9Vyi:
    - This is Bitcoin transaction **`d6b24ab29fa8e8f2c43bb07a3437538507776a671d9301368b1a7a32107b7139`**

What Is Bitcoin?

d6b24ab29fa8e8f2c43bb07a3437538507776a671d9301368b1a7a32107b7139

1FuckBTCqwBQexxs9jiuWTiZeoKfSo9Vyi (0.05 BTC - Output) 1FuckBTCqwBQexxs9jiuWTiZeoKfSo9Vyi (0.000016 BTC - Output) 1FuckBTCqwBQexxs9jiuWTiZeoKfSo9Vyi (0.00235018 BTC - Output) 1FuckBTCqwBQexxs9jiuWTiZeoKfSo9Vyi (0.00025497 BTC - Output)	1Ross5Np5doy4… (Free Ross Ulbricht) - (Spent)	0.05212115 BTC

0.05212115 BTC

Summary	
Size	763 (bytes)
Weight	3052
Received Time	2015-02-04 21:15:16
Included In Blocks	341974 (2015-02-04 21:16:58 + 2 minutes)
Confirmations	180240 Confirmations
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.05262115 BTC
Total Output	0.05212115 BTC
Fees	0.0005 BTC
Fee per byte	65.531 sat/B
Fee per weight unit	16.383 sat/WU
Estimated BTC Transacted	0.05212115 BTC
Scripts	Hide scripts & coinbase

d6b24ab291a8e812c43bb07a3437538507776a671d9301368b1a7a32107b7139

What Is Bitcoin Mining?

- It is the particular instance used to protect the transaction history for Bitcoin
  - Based on SHA-256
- Every miner takes all the unconfirmed transactions and puts them into a block
  - The block has fixed capacity (currently 1MB), limiting the global rate to ~3 transactions per second
  - Also attaches the "pay me the block reward and all fees" check to the front (the "coinbase")
  - Also attaches the hash of the previous block (including by reference everything in the past)
- Then performs the "Proof of work" calculation
  - Just hashes the block, changing it trivially until the hash starts with enough 0s.
    - This is the "difficulty factor", which automatically adjusts to ensure that, worldwide, a new block is discovered roughly every 10 minutes
- On success it broadcasts the new block

The Blockchain Size Problem

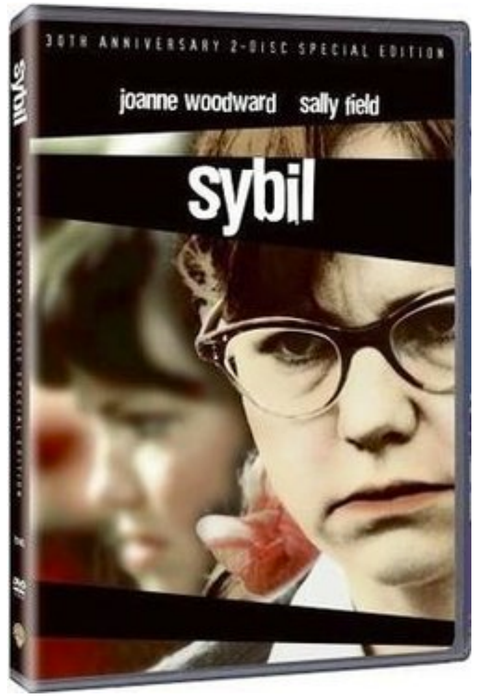
- In order to verify that Alice has a balance...
  - You have to potentially check ***every transaction*** back to the beginning of the chain
- Results in amazingly inefficient storage
  - Every full Bitcoin node needs access to the ***entire*** transaction history
    - Because the entire history is needed to validate the transaction
  - A "lightweight" node still needs to keep the headers for all history
    - And still has to ask for suitable information to verify each transaction it needs to verify
- So if we have 10,000 nodes, this means 10,000 copies of the Bitcoin Blockchain!

The Blockchain Power Problem

- The Bitcoin system consumes roughly 8 GW of power right now (or basically Austria!)
- This is because Proof of Work creates a Red Queen's Race
  - As long as there is potential profit to be had you get an increase in capability
  - Efficiency gains get translated into more effort, not less power consumption
- There is ***no way*** to reduce Bitcoin's power consumption without reducing Bitcoin's price or the block reward
  - It is this waste of energy that protects Bitcoin!

The Sybil Problem...

- There is a lot of talk about "consensus" algorithms in cryptocurrencies
  - How the system agrees on a common view of history
  - Bitcoin's is simple: "Longest Chain Wins"
- But Proof of Work is ***not*** about consensus:
  - It is about solving the sybil (fake node) problem...
    How do you prevent someone from just spinning up a gazillion "nodes"
    - Have each node have to contribute some resource!
  - "Proof of stake" is just another solution...
    Which requires your money to be easy to steal!
    Plus enshrines "he who has the gold, rules!"
- But there is an easier one: "Articulated Trust!"
  - Like the CAs: Use human-based agreements to agree on ***M*** trusted parties
    - Only ½***M***+1 need to actually be trustworthy!



The Irreversibility Problem

- A challenge: Buy $1500 worth of Bitcoin ***now***, without:
  - Needing $1500 cash in hand, transferring money to an individual, or having a preexisting relationship with an exchange
- You ***can't***!:
  Everything electronic in modern banking is by design reversible except for cryptocurrencies
  - This is designed for fraud mitigation: Ooops, something bad, undo undo...
- So the seller of a Bitcoin either must...
  - Take another irreversible payment ("Cash Only")
  - Have an established relationship so they can safely extend the buyer credit
  - Take a deposit from the buyer and wait a couple days

The Theft Problem...

- Irreversibility also makes things ***very*** easy to steal
  - Compromise the private key & that is all it takes!
- Result: ***You can't store cryptocurrency on an Internet Connected Computer!***
  - The best host-based IDS is an unsecured Bitcoin wallet
  - So instead you have hardware devices, paper wallets, and other schemes intended to safeguard cryptocurrency
    - It is worse than money under the mattress:
      Stealing money under the mattress requires ***physical access!***

The Decentralization Dream...

- "Trust Nobody"
  - The entire ***system*** is trustworthy but each actor is not
- Requires that there never be a small group that can change things...
- It is basically an article of faith that this is a good & necessary idea
  - But about the only thing it really buys is censorship-resistance

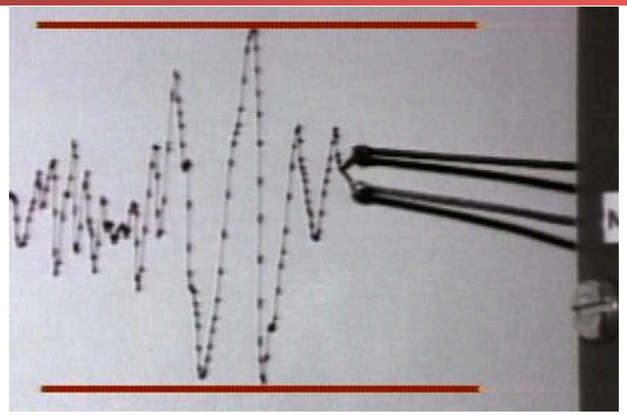
The Decentralization Reality

- Code is inevitably developed by only one or a few groups
  - And they can ***and do*** change it capriciously if it affects their money:
    When the Ethereum "DAO" theft occurred, the developers changed things to take ***their*** money back from the thief
    - Current debate to unlock another smart contract...
- Rewarded mining centralizes
  - Especially with ASICs and "Stealth ASICs" for proof of work mining
  - And the miners can ***and do cheat***, such as enable "double spending" attacks against gambling sites
- Several just aren't decentralized at all
  - Trusted coordinator or seed nodes
  - Ability to override/freeze assets

The True Value of Cryptocurrencies: Censorship Resistance...

- There is (purportedly) no central authority to say "thou shalt not" or "thou shouldn't have"
  - Well, they exist but they don't care about your drug deals...
- If you believe there should be no central authorities...
  - Cryptocurrencies are the only solution for electronic payments
- But know this enables
  - Drug dealing, money laundering, crim2crim payments, gambling, attempts to hire hitmen etc...
  - Ease of theft of the cryptocurrencies themselves
  - Ransomware and extortion
- And some minor "good" uses
  - Payments to Wikileaks and Backpage when they were under financial restrictions

Cryptocurrencies don't work unless you ***need*** censorship resistance



- ***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™
    - And thanks to the irreversibility problem, buying is expensive
  - But if you believe in the cryptocurrency, you ***must hodl!***

- Result is that the promised financial applications (cheap remittances etc) 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...
  - Otherwise, use PayPal, Venmo, Zelle, MPasa, Square, etc etc etc...

Worse:
Censorship Resistance Enables Crime

- Before the cybercrooks had Liberty Reserve and still have Webmoney...
  - But Liberty Reserve got shut down by the feds (a shutdown that ***really*** screwed up the black market hackers), and WebMoney is Russia-only
- So the only censorship alternative is cash
  - Which requires mass ($1M ≅ 10 kg) and physical proximity
- So the cryptocurrencies are the only game in town!
  - The drug dealers hated Bitcoin in 2013, and hate them all still, but it is the only thing that works
  - Ransomware used to be Green Dot & Bitcoin, but Green Dot was forced to clean up its act

And "Stablecoins" are no better...

- Removing the two currency conversion steps requires ***eliminating*** volatility
- Building a stable cryptocurrency requires an entity to convert dollars to tokens and vice versa ***at par***.
  AKA a "Bank" and "Banknotes"
  - Thus a centralized entity, so why bother with a "decentralized" blockchain? 🤔
  - All other "algorithmic stablecoins" are snake oil that implode spectacularly
- There is now a choice for the bank
  - Either you become as regulated as PayPal & Visa
  - Or you have a "wildcat bank"
  - Or you have "Liberty Reserve" and the principals end up in jail

Liberty Reserve

Department of Justice

Office of Public Affairs

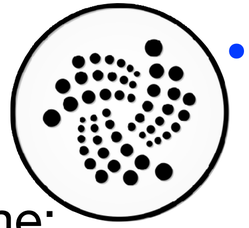
FOR IMMEDIATE RELEASE — Friday, May 6, 2016

Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions of 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 once used by cybercriminals around the world to launder the proceeds of their illegal activity.

Practically Every Cryptocurrency is "Me Too" with some riff...

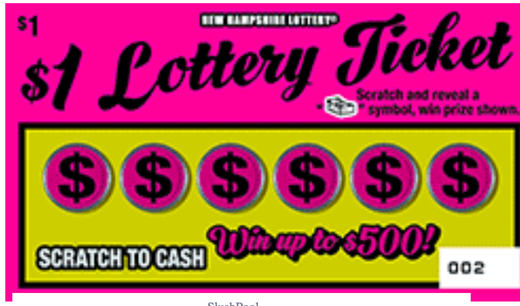
- There are lots of cryptocurrencies...
  - But in many ways they act the same: A public ledger structure and (perhaps) a purported decentralized nature
- Litecoin:
  - Bitcoin with a catchy slogan
- Dogecoin:
  - Bitcoin with a cool joke
- Ripple:
  - (Centralized) Bitcoin with an ***unrelated*** settlement structure

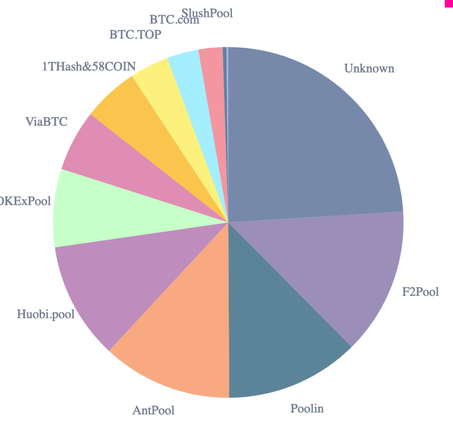


- IOTA:
  - (Centralized) Bitcoin but with trinary math 🤷 and roll-thy-own cryptography 🤦?!?!
- Monero:
  - Bitcoin with some better pseudonymity
- Zcash:
  - Bitcoin with ***real*** anonymity
- Ethereum:
  - Bitcoin with "~~smart contracts~~", unlicensed securities and million dollar bug bounties

Public Blockchain's Weak Security Guarantees

- "Public blockchains" protected by proof-of-whatever promise a "no central authorities" & "fully distributed trust" append-only data structure.
  - But this isn't the case!
- Any lottery-based reward creates mining pools
  - Which means a few entities ***can and do*** control things:
    3 entities effectively control Bitcoin with >50% of the hashrate
- The code developers also ***can and do*** act as central authorities
  - When ~10% of Ethereum was stolen from the "DAO", the developers rolled out a fork to undo the theft
- ***And worse...***



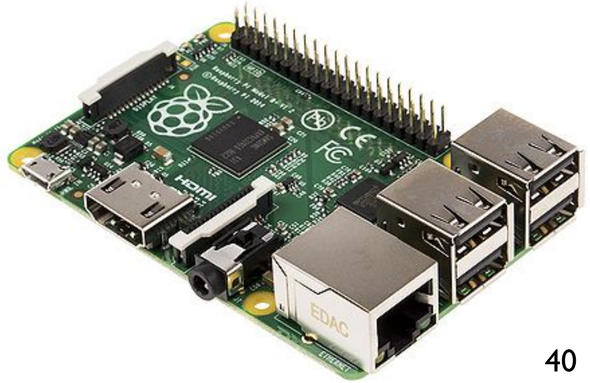


Proof of Work's Economic Unsoundness

- Idea: The system wastes $***x*** per hour to defend against potential attackers
- If an attacker needs to change the last ***n*** hours of history...
  - They will need to spend at least $***nx***, which acts as a floor
- This puts a ceiling on security as well: an attacker doesn't need to spend much more than $***nx***
  - If an attacker can make more than $***nx*** for an attack, they will!
- And its grossly inefficient:
  - The system is wasting $***x*** per hour ***whether or not it is under attack***
- Oh, and there are services!

So The Security Must Be Either Weak or Inefficient

- Proof of work is provably wasteful
  - It ***may*** be possible to make "proof of stake" work, but that has different problems
- And there is no way to make proof of work cheap!
  - Proof of "whatever" protects up to the amount that "whatever" costs, ***but not more!***
- So "articulated trust" is vastly cheaper
  - Take 10 trustworthy entities, each one has a Raspberry Pi that validates and signs transaction independently
    - In the end, 6 need to prove to be honest, but could easily process every Bitcoin transaction
  - This requires 100W of power and $500 worth of computers!, or 9 ***orders of magnitude less power***



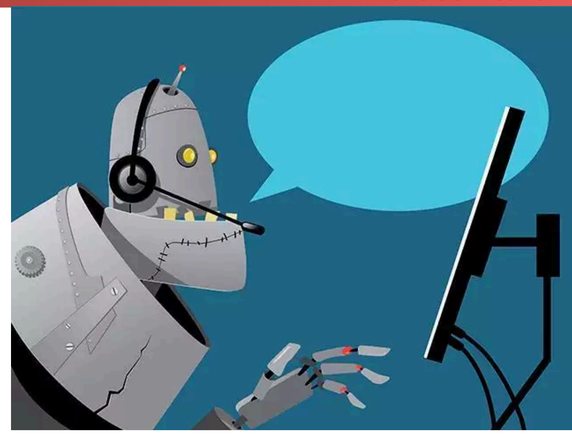
What About Non-Currency Blockchain Applications?

- 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

But There Is One Innovative New Stupidity: "Smart Contracts"

- Idea! "Contracts are expensive!" 🤔
  - So lets take standard things written in a formal language ("Legaleze")
  - And replace them with things written in a horrid language (that looks vaguely like JavaScript)
    - By default these "smart contracts" are fixed once released!
    - And this makes things cheaper ***how***?
- And ditch the exception handling mechanism
  - If you can steal from a Smart Contract, are you actually violating the contract?

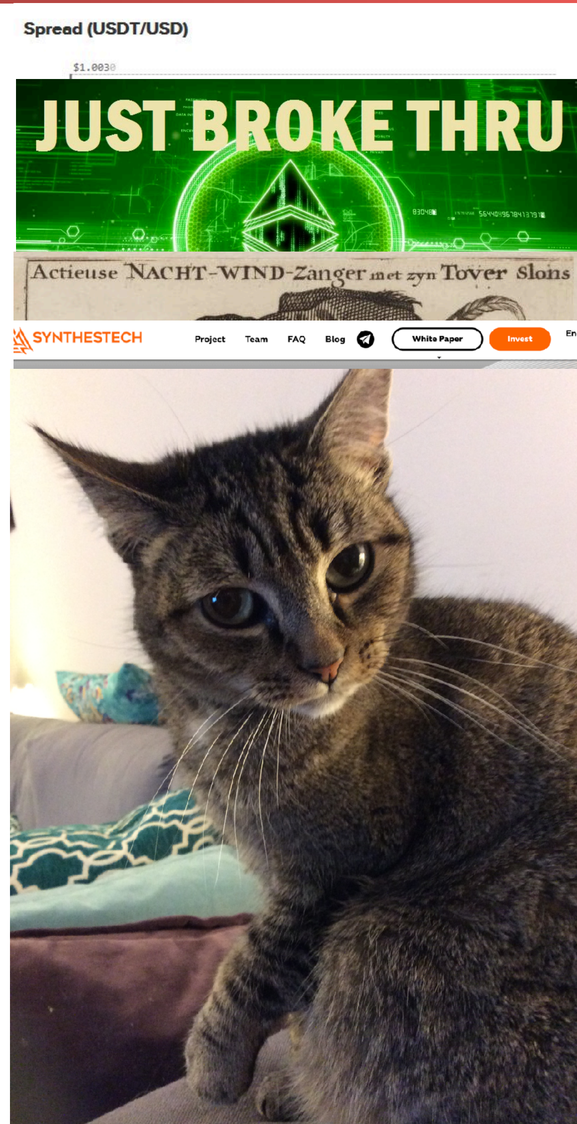
"Smart Contract" Reality: Public Finance-Bots



- They are really Public Finance-Bots
  - Small programs that perform money transfers
    - Finance bots are ***not new***:
      The novelty is these finance bots are public and publicly accessible
    - Oh, and these aren't "distributed apps"
- Predictable Result: Million Dollar Bugs
  - The "DAO", a "voted distributed mutual fund as smart contract":
    Got ~10% of Ethereum before someone stole all the money!
  - The "Parity Multi-Signature Wallet" (an arrangement to add multiple-signature control to reduce theft probability)
  - The "Proof of Weak Hands 1.0" explicit Ponzi Scheme

The Rest Is Speedrunning
500 years of bad economics...

- Almost every cryptocurrency exchange is full of frauds banned in the 1930s
- Ponzi schemes without postal reply coupons, including explicit ponzies as "Smart Contracts"
- Tether, a "stablecoin" is almost certainly a wildcat bank from the 1800s
- Every tradable ICO is really an unregulated security just like the plagues in the South Sea Bubble of 1720
- Replicated rare tulips with rare cats on the Ethereum Blockchain as a "Smart Contract"! Time to party like it is 1637!
- And don't forget the goldbug-ism...



Smart Contracts and "Decentralized Finance": Speed Running the Speed Run

- "Hey, only Wall Street has previously benefitted from super-whiz-bangie techno innovations"
  - So lets instead build them as "Smart Contracts"?
- ONLY applications end up being:
  - Fraudulent stocks (ERC20 tokens)
  - Tulip Manias
  - Implicit ponzi schemes ("Yield Farming")
  - Explicit ponzi schemes