Blockchains and Cryptocurrencies

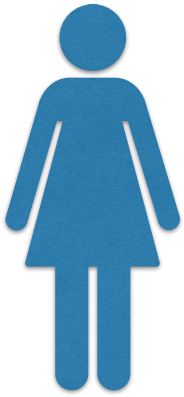
Why This Lecture?!?

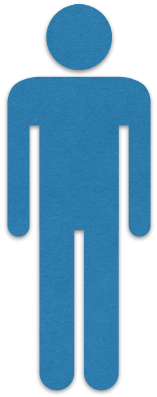
- I am an actual ***expert*** in this area
  - It has been one of my research focuses for the past 5+ years!
- But I want it to die in a fire!
  - There is effectively no value:
    - Private Blockchains are 20+ year old ideas
    - Public Blockchains are grossly inefficient in the name of "decentralization" 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

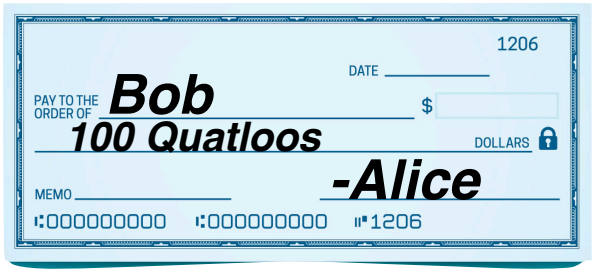
What Is A "Cryptocurrency"?

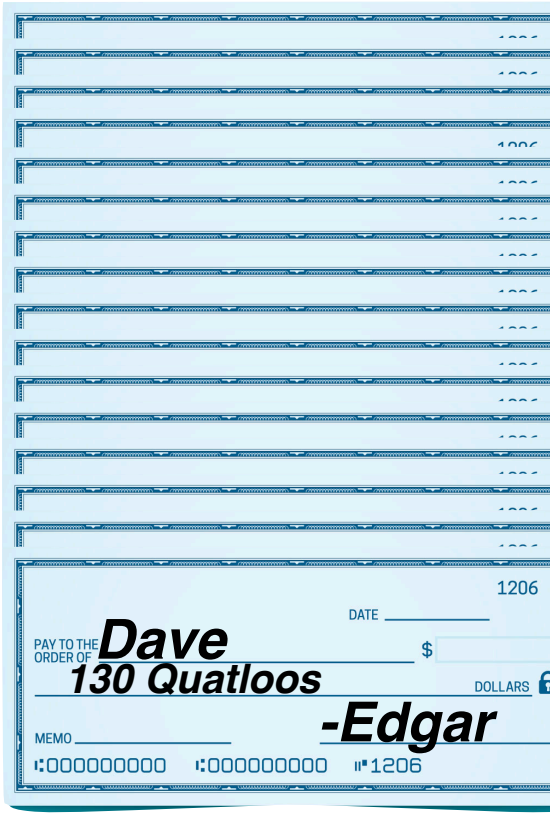
- A cryptocurrency is a tradable cryptographic token
  - The goal is to create irreversible electronic cash with no centralized trust: If Alice wants to pay Bob 200 Quatloos to pay off her losing bet on the Green thrall, there should be ***nobody else who can block or reverse this transfer***
- Based 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"?





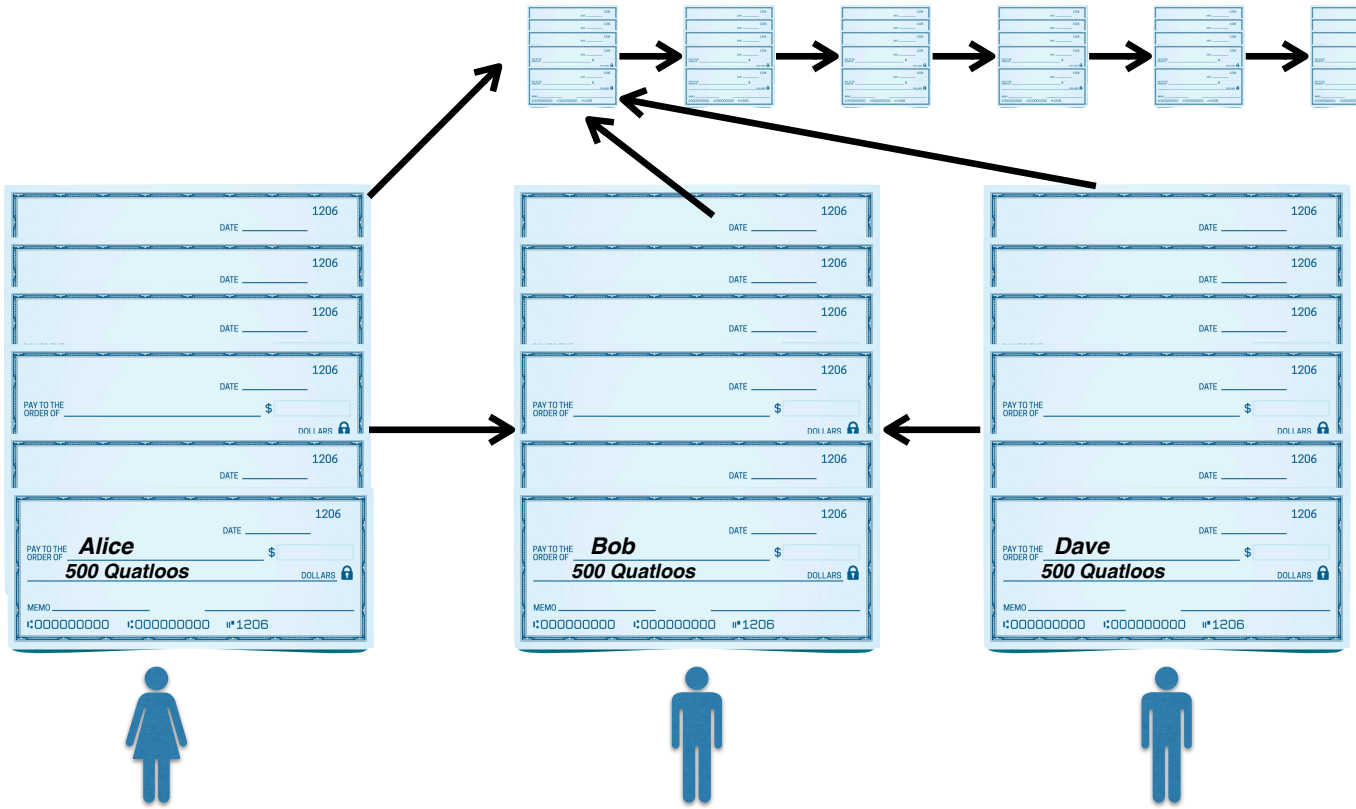




What Is A "Blockchain" (well, "Public" or "Permissionless" Blockchains)

- 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
    - Public key signature: A function pair:
      - ***Sign(X,K_{priv}) -> Y*** (can only be done if you know K_{priv})
      - ***Verify(X,Y,K_{pub}) -> True/False*** (can be done by anybody who knows K_{pub})
  - 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

What Is Bitcoin Mining?

- It is the particular instance used to protect the transaction history for Bitcoin
  - Based on a cryptographic hash function, which looks "random" and is irreversible
- 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

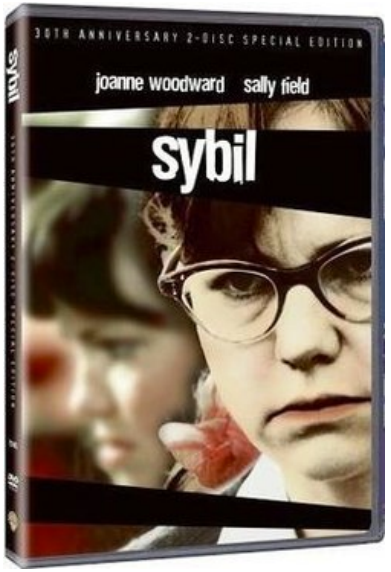
- In order to verify that Alice has a balance...
  - You have to potentially check ***every transaction*** back to the beginning of the chain
- Results in amazingly inefficient storage
  - Every full Bitcoin node needs access to the ***entire*** transaction history
    - Because the entire history is 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, ***at minimum***, 10 GW of power right now (or as much as New York City!)
- 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!
- 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

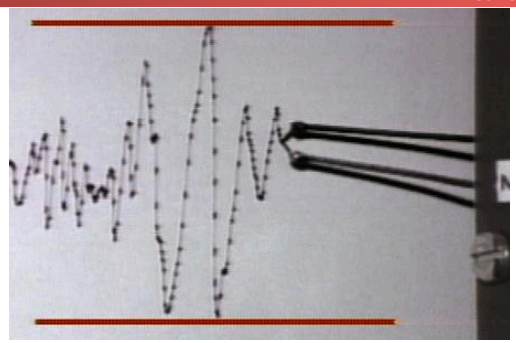
The Decentralization Reality

- 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
- https://arewedecentralizedyet.com

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

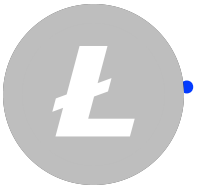
Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE Friday, May 6, 2016

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

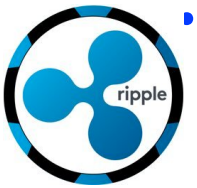
Arthur Budovsky, 42, was sentenced today in the Southern District of New York to 20 years imprisonment for running a massive money laundering enterprise through his company Liberty Reserve S.A. ("Liberty Reserve"), a virtual currency once used by cybercriminals around the world to launder the proceeds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

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

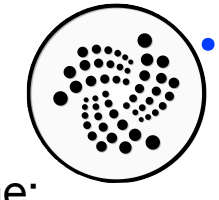


- There are lots of cryptocurrencies...
  - But in many ways they act the same: A public ledger structure and (perhaps) a purported decentralized nature
- Litecoin:
  - Bitcoin with a catchy slogan

- 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 🤦?!?!

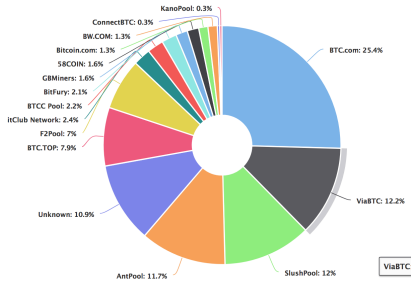
- Monero:
  - Bitcoin with some better pseudonymity

- Zcash:
  - Bitcoin with ***real*** anonymity

- Ethereum:
  - Bitcoin with "~~smart contracts~~", unlicensed securities and million dollar bug bounties

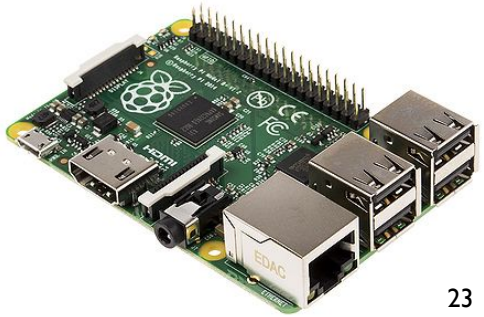
Public Blockchain's Weak Security Guarantees

- "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
- ***NO significant cryptocurrency/public blockchain is decentralized***!
  https://arewedecentralizedyet.com/



And 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 8 ***orders of magnitude less power***



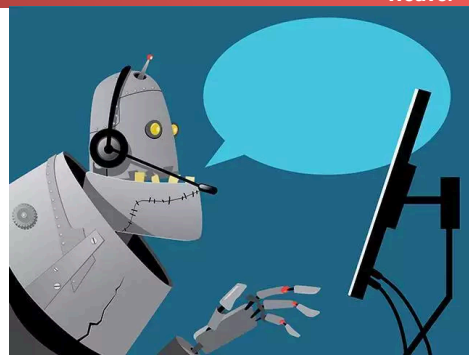
What About Non-Currency Blockchain Applications?

- 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?

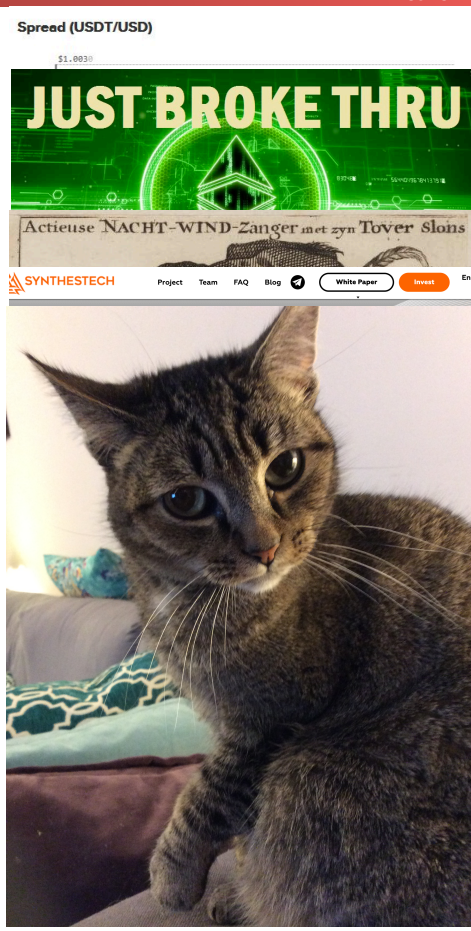
"Smart Contract" Reality: Public Finance-Bots



- 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 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!
- And don't forget the goldbug-ism...



More On "Initial Coin Offerings"

- The Loud Part: "Hey, anyone can buy this cryptographic token that can be exchanged for future service X or just a future cryptocurrency"
  - And we will now perhaps build X using all the money you give us (trust us, we have a whitepaper)
- The Quiet Part: "You can then trade that token on an exchange, because someone might want to pay more for the service"
  - Which makes this really an unlicensed, unregulated security
- With predictable results
  - Effectively 100% failure rate to-date for any service other than a cryptocurrency itself
  - Massive amounts of scams and frauds...
    ANY ICO not limited to accredited investor should be considered a criminal scam
  - Most ICOs these days are meta-tokens: They don't even create a new "blockchain" but run on an existing system like Ethereum

What's The Prescription?
Fire, and ***lots of it***

- Individual:
  - Fortunately, there is little ***systemic*** risk in this area. So feel free to ignore it or point & laugh
- Blackhats: ***Worms***
  - Massive theft of cryptocurrencies for fun and ***profit***!
- Government: ***Enforce the Laws***
  - Target Bitcoin Exchanges
  - Target Private Transfers
  - Target Tether
  - Target Fungibility
- Government or others: ***Technical Disruption***
  - Drive undesired blockchains into the ground with spam

Calling All Blackhats: Release ~~The Kraken~~, err Worms!

- Worm: A self propagating malicious program
  - Starts running on one system... From there it spreads exponentially by infecting other vulnerable machines
- Cryptocurrencies are a glorious target for ***profitable*** worms
  - Cryptocurrencies are trivial to steal if online: Get the private keys and shift the money
  - Cryptocurrency speculators often have multiple cryptocurrencies on the same system...
  - Peer to peer systems support ***very fast*** worms: Worldwide spread in seconds!
  - Many "zombie coins" out there which make weak targets
    - Dogecoin is still worth $1B, but no updates in 3 years and a fork of a fork of a fork written in C++!
    - Even ***new from scratch*** such as the Bitcoin "Lightning" network is in C++

So How To Make Money In Cryptocurrencies...

1. Move to Sochi (unless you already live in Pyongyang)
2. Find a Remote Code Execution exploit in a top 100 cryptocurrency
3. Make this exploit robust
4. Write a payload that looks for all major cryptocurrency wallets, stealing the wallets (if encrypted) or just the money (if unencrypted)
5. Include a keylogger which automatically tries to use entered passwords to decrypt local wallets
6. Combine the payloads and exploit with a framework that searches for more victims in the p2p system
7. Release your worm and watch the money roll in!

Government Target #1: Exchanges...

- Bitcoin Exchanges should have a choice
  - Follow anti-money-laundering laws ***and*** consumer protection laws ***and*** security laws ***and*** full reporting to the IRS like a brokerage firm ***and...***
  - Be completely cut off from all international banking connections: Not just the US but Europe & Japan (many are already this way)
- Goal is to protect consumers, block criminality, and eliminate all of the cost "savings" that only exist due to regulatory avoidance instead of actual innovation
  - If this bankrupts Coinbase, 🤷

Government Target #2: Local Bitcoins...

- A key enabler of criminality (especially drug dealers) is the ability to turn Bitcoins into $ and vice versa
- Effectively ***every*** significant participant selling Bitcoin on LocalBitcoins is committing felonies involving unlicensed money transfer
  - So treat them like drug dealers
- Doubly effective:
  - If you treat them like drug dealers, it costs like buying drugs: attacks the utility as a currency
  - And gives you convenient hooks into investigating larger criminal networks

LocalBitcoins.com
Instant. Secure. Private.

Government Target #3: Tether

- Tether is an ***allegedly*** stable cryptocurrency
  - Promises a 1-1 tie to US dollars to the tune of ~$2B
  - Almost certainly a "wildcat bank"
  - If not, its Liberty Reserve Mk 2
  - ***Either way*** it is almost certainly a criminal enterprise
- The unbanked exchanges ***rely*** on Tether
  - The speculative traders need to go from "unstable" to "stable" and vice versa
  - A huge fraction of the "Dollar" volume for Bitcoin on exchanges are actually “Tether"
  - Strong research suggests that Tether is the reason for the price rise

What Does Destroying Tether Get?

- It not only removes a $2B bad-actor...
- It removes the value proposition for the unbanked exchanges: Participants could no longer trade volatile for "stable", but only volatile for volatile. And these exchanges are >80% of the Bitcoin market!
- These exchanges are also effectively criminal enterprises:
  - They offer trading platforms for unlicensed securities
  - They accept ***payment*** from unlicensed securities for listing
  - They ***do not*** follow the laws about stopping money laundering
  - They are the support for "privacy" coins which are designed for money laundering
- So don't play whak-a-mole on the exchanges... just whak their business model

Government Target #4: Fungibility

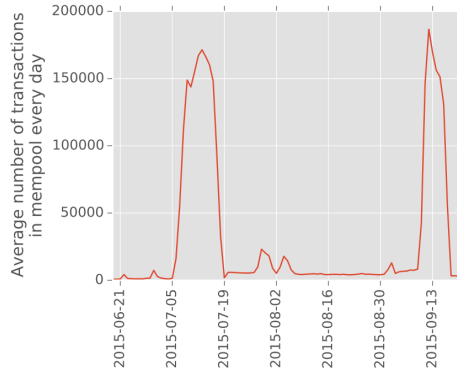
- *Pecunia non olet*: "Money Does Not Stink"
  - It should be impossible to determine the previous history of a coin: Otherwise not all coins are the same anymore (fungibility)
  - But Bitcoin is ***insanely*** traceable
- So why not attach a "stink" to cryptocurrencies?
  - Cryptocurrencies which are pseudonomous: Require legal exchanges to seize known-dirty money
  - Cryptocurrencies which are truly anonymous: Is there a reason to allow legal exchanges to support something designed for money laundering?

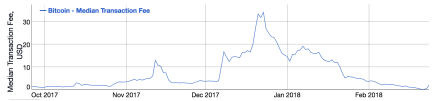
Ross Anderson et al's Proposal: FIFO Taint

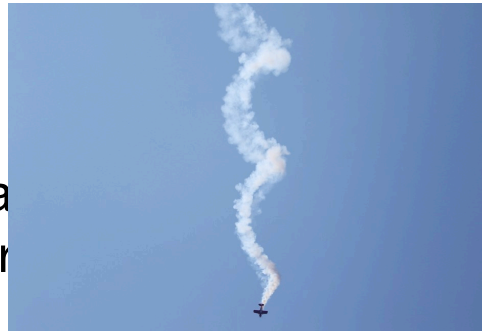
- Its easy to taint & trace Bitcoin from known-bad sources
  - Thefts, drug markets, etc etc etc...
  - But taints spread too much: coins quickly end up "2% bad" or suchlike
- Anderson proposal:
  The tainted output of a wallet is a FIFO
- Require legal Bitcoin exchanges to respect FIFO taint
- Taint major criminal activities
- Sell it as handling theft...
  But the reality is an attack on all cryptocurrencies!

Technical Target:
Limited Capacity Fee Death Spirals

- If # of transactions < capacity
  - Transactions may be cheap...
  - Including cheap for spammers who want to occupy space ***foreve***
- If # of transactions > capacity
  - Fee auction death spiral:
    Price/transaction goes from ~$0 to $30+
  - Only those willing to pay see their transactions processed
- Phase change can be sudden and painful
  - And even profitable: A mining pool could benefit from triggering a
    Clog their own blocks with "pay to self spam" when there is other
    capacity.







Exploiting The Death Spiral: The $1M Plan to Destroy a Cryptocurrency

- Either option is ***exploitable*** by a moderately-funded adversary
- Spam the target blockchain whenever below the death-spiral point
- Just grab the popcorn whenever it is above the death-spiral point
- If the block size goes up...
  Your spam just occupies even more space! ***FOREVER***!!!!
- If the block size stays constant...
  The system keeps becoming unusable whenever you want it to be
- And ***when*** they install spam filters...
  - Tune your spam to cause false positives:
    Autoimmune disease (on the Blockchain!)
- Result: Cryptocurrency ceases to be reliably exchangeable

So Where Does This Leave Us?

- The Cryptocurrency & Blockchain space is...
  - And should be avoided at best, and really needs to just die in a fire
- But it is also remarkably ***weak***!:
  So here are the matches & gasoline:
  - Knowledge can immunize you from the field
  - Blackhats can make a fortune from mass theft
  - Governments can destroy the utility using existing regulation
  - Anyone willing to spend a moderate amount of money could destroy Bitcoin or other targeted cryptocurrencies with spam