



ENIGMA

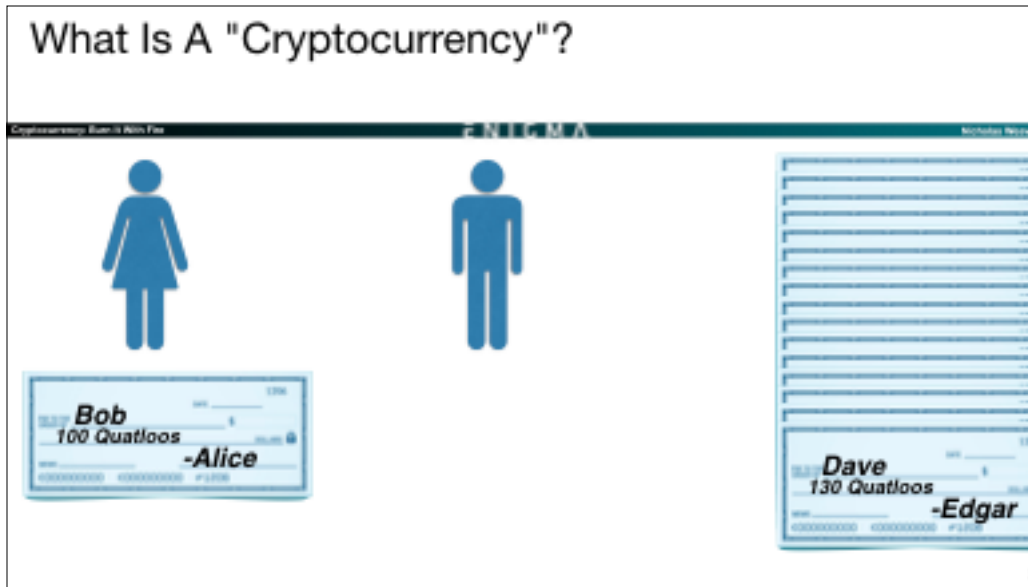
Cryptocurrency:
Burn It With *Fire!*
Nicholas C Weaver



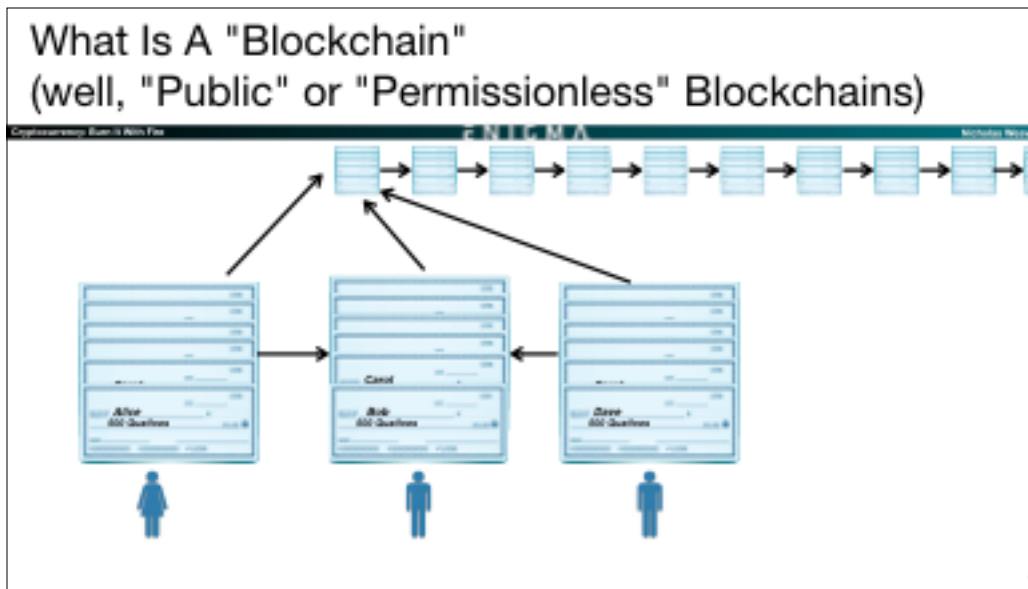
Hi, I'm Nick Weaver and I'm here to talk about cryptocurrencies. My work in the area is largely sponsored by the National Science Foundation, however all opinions are my own. This is also not investment advice, but then again, I think anyone who advises you to invest in cryptocurrencies should just be kicked in return.

I've been researching and writing in this space academically [{click}](#), as well as for general interest publications for over 5 years now. And I've suffered for my exposure. Most others who've followed this space for this long are true believers, as almost everyone else who looked at it at the start and went "This is BS" walked away. But I have a monetization model that allowed me to continue to watch it: I got to mine comedy gold and turn it into papers and essays.

And it also appears that the space is finally burning down [{click}](#), as it has well deserved to. So this may prove to be a bit of dancing on some graves.



The goal of a cryptocurrency is to create **irreversible electronic cash with no centralized authorities**, so that nobody else can block or reverse a transfer. So let's say Alice wants to pay Bob 100 Quatloos for a winning bet on the Green Thrall. She basically writes a check, cryptographically signs it, and hands it to Bob. {click} But is the check any good? Well, there is a public ledger of all previously cancelled checks {click}, so we can check if Alice has a balance. Assuming she does, the check is good and the check is now added to the global ledger {click}, showing that Alice is now down 100 Quatloos and Bob is up 100.

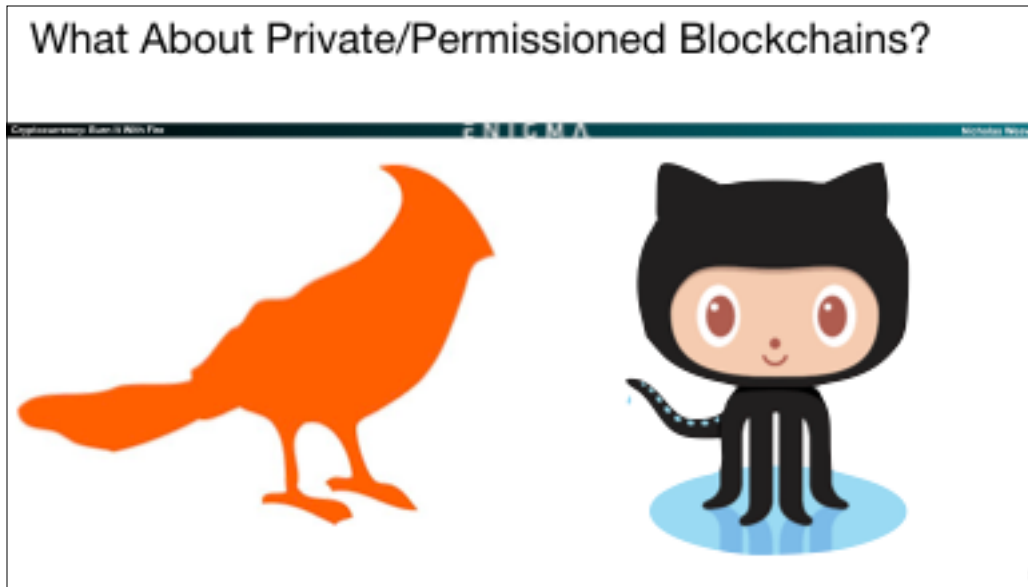


So how do we build this ledger? Enter the “blockchain”. A **blockchain is simply a hash-chain**: so each bundle of cancelled checks includes the cryptographic hash of the previous bundle. Since **cryptographic hashes are effectively unique and untamperable identifiers**, if we know the most recent bundle is valid we can know that the previous bundle is valid, and then the previous bundle from there, going back to the beginning. This creates an “**append only**” data structure, that is, we can only add new entries.

So how do we add new entries? {click} Well a whole bunch of participants, the “miners” in cryptocurrency parlance, gather up all the new checks, ensure they are valid, add a “pay to myself” check for all the work they are going to do {click}, include a pointer to the previous block, and staple them together with a cryptographic hash into a block of new checks.

But in order to ensure that somebody can’t just play games, the hash has to be below a certain number, the “difficulty factor”. **If it isn’t, just tweak the “pay me” check until the hash is below the threshold**. Since hashes are also effectively random, this creates a proof of work system., as any hash below that value probably required producing a huge number of hashes.

So everybody keeps at it, until one person gets lucky. {Click} Now that bundle is part of the record and everybody now starts all over again with a new set of checks.




You will often hear proponents talk about a "**Blockchain Revolution**", and in it they conflate two totally different things. You have the **permissionless blockchains, which are supposed to be "decentralized" and "trustless"** (what this means and which they aren't we will see later), and which are only really used for the cryptocurrencies.

And then you have the "**permissioned**" or "**private**" chains, which are simply an append only data structure signed by one or a few trusted parties. And yes, such structures are useful, albeit 20 years old and called "hash chains" to you and me. But as a management consultant, stick that blockchain bird {click} on things and now idiots in management will throw money at you. Of course, real hash-chain based projects, such as certificate transparency efforts, don't bother calling themselves "blockchains".

So in the end this also means there will be no blockchain revolution, because anything that can benefit from append only record-keeping like that should already be in a Git archive{click} or other append-only structure. So for all those who say "Blockchain will solve X", the only thing it solves is you now know the person knows nothing about X.

What Is Bitcoin?



Blockchain Explorer

Transaction ID: [48d74e2994e4b0c3e07138807776d714801388a1c4d21070738](#)

1fuc8TCpr9Gee0pWt2aerYohy: 0.05 BTC - Output
 1fuc8TCpr9Gee0pWt2aerYohy: 0.00018 BTC - Output
 1fuc8TCpr9Gee0pWt2aerYohy: 0.0023018 BTC - Output
 1fuc8TCpr9Gee0pWt2aerYohy: 0.0025487 BTC - Output

0.05212115 BTC

Summary		Inputs and Outputs	
Size	763 Bytes	Total Input	0.05262115 BTC
Weight	3052	Total Output	0.05212115 BTC
Received Time	2015-02-04 21:15:15	Fee	0.0005 BTC
Included in Blocks	341974 (2015-02-04 21:15:58 + 2 minutes)	Fee per byte	65.531 sat/B
Confirmations	18040 Confirmations	Fee per weight unit	15.383 sat/WU
Visualize	View Tree Chart	Estimated BTC Transacted	0.05212115 BTC
		Scripts	Hide scripts & conf-base

And now we get to Bitcoin, which is simply the first widespread cryptocurrency. A **bitcoin “address” is simply the hash of an associated public key**, and the **bitcoin wallet** is a tool for holding the private keys. To spend Bitcoin, you simply create a check and cryptographically sign it with the corresponding private key, broadcast it to the network, and once the miners include it, it is now official and irreversible.

Why They Don't Work As Currency: Hard To Purchase



The first thing a currency needs to be able to do is actually be useful for paying for things. In this, all the volatile cryptocurrencies fail. By design, they are supposed to have no central authorities that could reverse a transaction. But that means they are fundamentally incompatible with the modern financial system, which depends on reversibility to mitigate fraud. Which makes cryptocurrencies hard to get.

This means if you are buying bitcoin you either need to {click} use cash, {click} be given credit by the seller, or {click} Transfer your money and then wait a while. Because if you don't, you end up like {click} this guy, who lost \$75,000 worth of Bitcoin when he sold them to someone who used PayPal, only to find days later that the credit card was stolen and the payment reversed.

Why They Don't Work As Currency: Harder To Hodl



Technology Intelligence
Bitcoin owners told to transfer savings out of Bitpay wallets after private keys stolen

Not only are the cryptocurrencies hard to buy they are even harder to hold.

You clearly can't store your cryptocurrencies with a third party, as they seem to be {click} hacked and implode with disturbing regularity. And unlike your bank which has government backed insurance, it is the depositors who lose the money.

But you should also never keep your cryptocurrencies on an internet connected computer, because they are so easy to steal. In fact, the best host based intrusion detection system {click} is simply a small unsecured Bitcoin wallet. In fact, we used this to detect an intrusion ourselves, when a thief broke into a graduate student's computer and among other things stole our honeypot wallet! And let that sink in. This is supposed to be the "Internet of Money", but you can't keep it on an Internet connected computer.

And finally even if you are using a secured device like a dedicated phone (because, lets face it, an iPhone is probably the most secure Internet-connected device you can buy), you have to trust the code that is managing your cryptocurrencies. {click} Which may be compromised when even something so minor as an open source module imported using NPM is compromised.

Why They Don't Work As Currency: Hardest To Spend



Finally, there is how you spend your cryptocurrency. The merchant you are buying from is almost inevitably using a service that {click} allows them to price in Dollars and which converts to dollars automatically, so they aren't exposed to the volatility risk {click}. Which means the buyer, unless they want exposure to that volatility, has to go through the difficult purchase problem. As a result, real world cryptocurrency transactions, when you include two separate currency conversion steps, are far more expensive than the alternatives such as Visa, PayPal, Venmo, M-Pasa, Zelle, Western Union, etc...

The only exception that doesn't require two currency conversion steps is if you are a believer in the cryptocurrency and therefore have been holding onto it. But these things are designed to be deflationary, so your money is worth more tomorrow than it is today. For those who skipped Econ 1, this is effectively recapitulating the gold standard, where some fixed supply of money is built into the system. Unfortunately the gold standard was an abject failure as seen in the great depression. And we see the same failure mode in Cryptocurrencies. Because the first rule in a deflationary environment is never spend your money, lest that 10,000 Bitcoin {click} pizza purchased in the early days of Bitcoin fill your belly with regret if the value of the cryptocurrency shot up to the moon.

So What's The Purpose: Censorship-Resistance For Crime



So what good are the cryptocurrencies? Well, the one thing they have that isn't present in other electronic payments is "censorship resistance", there is no authority which blocks illegal transactions. So naturally, this is the money of crime. Not just {click} drug dealers, but of greater importance is it is the money of extortion, whether you are threatening people with {click} the loss of their data, revealing secrets, or even the latest: bomb threats.

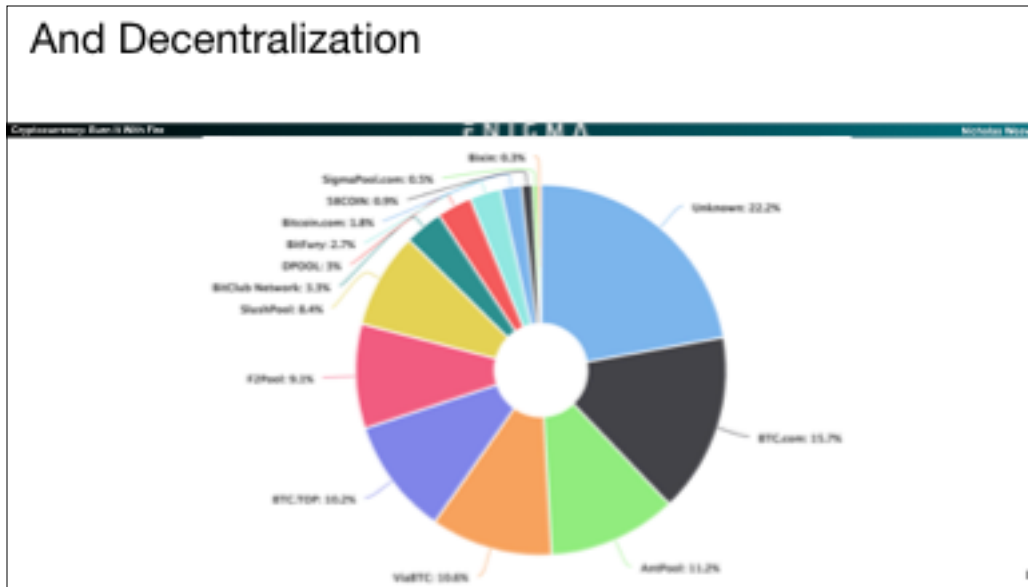
Of course, this does get used for legitimate businesses that are otherwise blockaded. For example, until Wikileaks arranged with a US nonprofit to get around Visa' blockade, {click}, it was a way of contributing to the alleged rapist in the Ecuadorian embassy. It was also used by Backpage {click} for those who wanted to post personals when Visa and Mastercard stopped service. Oh wait, that was also a {click} criminal enterprise.



But as a final bonus, they can't be both efficient and secure. You see, that whole "proof of work" business is not about securing "consensus", a global view of what the network should be, but rather preventing sibyls: stopping someone from just creating a gazillion fake nodes and getting a gazillion votes. So it works under the assumption that an attacker won't burn more money than the network already is. Which is fine security if you're willing to burn Joker-stacks of money {click} to verify three transactions a second.

Of course, if you explicitly stated "these are the 10 trustworthy entities, 6 must be honest responsible for history", making it an old-school "private" blockchain, you could do the same thing on 10 Raspberry Pis {click} using less power than an incandescent light bulb!

Yet if you don't waste an obscene amount of resources, these proof of work systems are insecure. Thus small "alternate" cryptocurrencies using proof of work are regularly attacked {click}. And there is even a service {click} that allows an attacker to easily recruit the computing needed.



One other thing you hear a lot of in the cryptocurrency space is "decentralization", the idea that the system is distributed across a huge number of computer and, in that process, you only are supposed to trust the system in aggregate, not individual players and there are no central authorities in the supposedly "trustless" system.

But overall the benefits of decentralization are generally believed without support rather than something articulated, and except for the censorship resistance there is generally a failure to articulate why decentralization is somehow superior to having a more conventional system with trusted parties, federated agreements, and other conventional solutions where you articulate who the trusted parties are.

And the things centralize all the time anyway: {click} Mining is performed by a few cartels, basically eliminating any hypothetical decentralization. The coders are also central authorities as we will see later.

Only One Financial "Innovation": Smart Contracts



```
Contract Source Code in
184 //
185 //
186 //
187 event onTokenPurchase()
188 address indexed customerAddress,
189 uint256 lockedEtherSum,
190 uint256 tokenSum
191 }
192
193 event onTokenSell()
194 address indexed customerAddress,
195 uint256 tokenBurned,
196 uint256 etherSumSold
197 }
198
199 event onInvestment()
200 address indexed customerAddress,
201 uint256 etherSumInvested,
202 uint256 tokenSumSold
203 }
204
205 event onWithdraw()
206 address indexed customerAddress,
207 uint256 etherSumWithdrawn
208 }
```

Overall, the field is largely devoid of economic innovation, except for one idea you've perhaps heard of, "Smart Contracts". The vision is simple, take things written in a formal language {click} colloquially called legaleze, rewrite them into a language that {click} makes JavaScript seem sane, and ditch the exception handling mechanism, the courts, {click} which is invoked when things go wrong. How rewriting standard contracts is supposed to save tons of money is left up as an exercise to the listener, because I can't see how that would work. And ditching the exception handling mechanism is a huge cost, because if you can steal from a smart contract due to a bug in the code, is it actually theft?



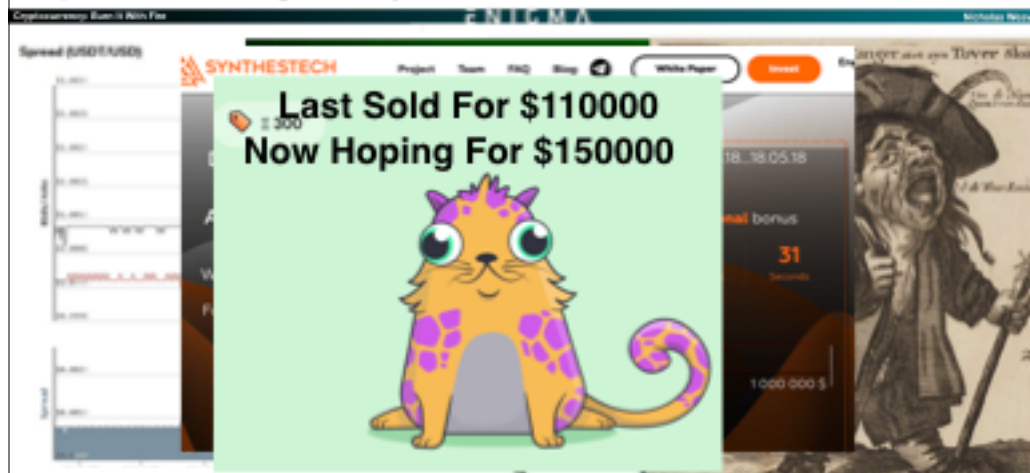
Of course, the reality is much more prosaic: These are finance bots {click}, small programs that act on money. Finance bots are an old idea: your index funds for example are run by such bots. The difference is these bots are public, {click} so anyone can interact with them. The result is a cavalcade of failures.

The first, {click}, the DAO, or "Decentralized Autonomous Organization", was a distributed mutual fund idea. Roughly 7% of all Ethereum flowed into it before a hacker realized they could take the money out due to a reentrancy bug. And then the Ethereum developers showed that the whole "code is law" and "decentralization with no central authority" business is an outright lie by changing the code behind Ethereum to undo the theft, since it was their money stolen.

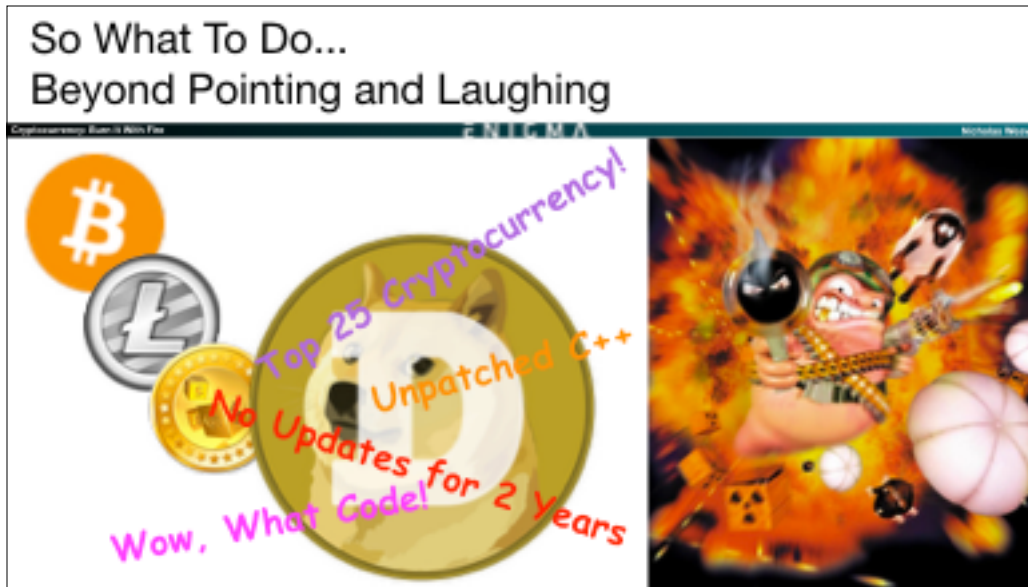
Then there was {click} the Parity wallet. This was designed to keep your money safe, allowing you to require multiparty checks. Unfortunately, there was a bug where someone could go "hey, wallet, gimme all the money", and it did. This theft was limited, because a good "robin hood" stole most of the money and returned it to the victims. The next version had a different bug, where someone went up to the master library for the wallet and said "hey, you belong to me, now delete yourself", making some \$100M at the time permanently inaccessible. Of course, the bonus is the lead behind Parity is the guy who invented Ethereum's smart contract language!

Finally we had the "Fear of Missing Out" Ponzi scheme {click}. This was a ponzi scheme with a twist: Although early people got paid as contributions went in, the LAST to contribute would get the bulk of the prize pool. So someone did a contribution and then simply clogged the Ethereum network with high-paying spam, until the contract said "OK, you won" and gave the attacker the money!

Everything Else: Speedrunning 500 years of Economic Failures



Everything else is speed running a half millennia of economic failure, from recapitulating gold-bugism, to [blatantly manipulated markets](#), to ["fair" ponzi schemes](#) and [fraudulent stocks touted by celebrities](#) (Anyone want Alchemy on the Blockchain? [to even tulip bulbs in the form of digital cats](#)), where someone bought "ownership" of this fine specimen simply because he was hoping someone else will pay even more.



So what to do?

First, these targets are ripe for attack. Take as just one example Dogecoin. It is a peer to peer cryptocurrency that is a {click} fork of a fork of a fork, with the code starting at Bitcoin, branching off for Litecoin, then Luckycoin, and finally dogecoin. Why does this matter? {click}

You have a peer to peer system that is unpatched C++ and no updates for 2 years, and we all know that people do store multiple cryptocurrencies on the same computer. So if someone in say Sochi or Pyongyang {click} wanted to write a cryptocurrency stealing worm, a self propagating malicious program spreading through the Dogecoin network, it could sweep through that entire network in a matter of seconds, and then immediately steal all other cryptocurrencies it can access.

And Enforce The Laws!



Second is actual law enforcement. The amount of criminality in the space is simply off the hook. Now the US government generally avoided getting involved, I think for fear of being accused of "stifling innovation". But now that things are collapsing, they are waking up. The IRS has subpoenaed cryptocurrency exchanges. The SEC now has a standard ICO settlement template. The CFTC is starting to look at exchange manipulation.



Finally, these systems are vulnerable. Back in 2015 [{click}](#) someone spent a modest amount of money to just shut down Bitcoin. And in late 2017 the Bitcoin network hit a capacity limit which caused fees to [{click}](#) enter a death spiral, so if you wanted your transaction to go through you had to outbid everyone else,

This is exploitable. Someone could spam the network whenever its below the death spiral point, shutting it down at will. And when it is above, do nothing but laugh. [{click}](#).

Keep this up until the network installs spam filters, and then the attacker starts a more interesting game: tuning spam not to get through the filters but to have the filters trigger false positives. How well would a currency work if 1-2% of transactions are randomly blocked by spam filters?

Ethereum seems a particularly ripe target, with a full blockchain of over 2TB and working sets measured in the 100s of GB. What happens if an attacker adds a 0 or two to those numbers?

Conclusions...



In the end, it is a dismal space. Private and permissioned blockchains are simply an old idea with a new buzzword. Public blockchains are grossly inefficient. Cryptocurrencies don't actually work unless you want to buy drugs. Smart Contracts are a disaster. And the field is just recapitulating 500 years of failure. So in the end, the only winning move is not to play. Unless that is you like playing with a flamethrower {click}

But What About "Stablecoins"?



Finally, you may have heard about "stablecoins", cryptocurrencies that are designed to not bounce around in price but instead maintain a fixed value. One common option is just backed by money. But in that case, why not just use Visa, since the stablecoin should be equally regulated. Of course, such stablecoins could actually be fraudulent and not actually backed up. And those behind the stablecoin have to watch out, because they can go to jail. Liberty Reserve was an online currency, albeit without a blockchain. So effectively a stablecoin with a more efficient centralized database. Those behind it were prosecuted because they turned a blind eye to money laundering.

An alternate design involves backing the stablecoins with cryptocurrency. This is all fine and good only as long as the cryptocurrency only goes up. Finally there have been some particularly bonkers ones with algorithmic "central banks". Fortunately for them, they gave up realizing their project was illegal before they found out that if you have a currency peg and someone can figure out how to make money breaking it it will be broken.

{Move to backup}

But What About Proof of Stake?



If you follow this space you do hear about an alternative to proof of waste systems, usually premised on "proof of stake": By having a lot of the currency already you can validate new transactions {click}. Of course there are a few problems with this. First, remember how you are not supposed to keep your cryptocurrency on an internet connected computer? {click} Yeah, that. Then there is the recapitulation of feudalism {click}, where those with the gold make the rules since the more money you have the larger your vote. Does having the most money give the biggest vote really make sense in systems with greater inequality than north korea? Does that count as "decentralized"? It often ends up being proof of work in disguise. And finally it is often {click} vaporware: something seemingly continuously promised but really not delivered on as anyone who's followed the Ethereum saga can tell you.

Truth be told, if your system already assumes that secure enclaves are secure {click}, just use the secure enclaves to prevent sibyls: Each hostile node would cost a full CPU. And, oh yea {click}, SGX got broken too. SGX is a good seatbelt when you sorta-trust the other parties, not something I'd rely on really working in a purely malicious environment.