DSHR's Blog

I'm David Rosenthal, and this is a place to discuss the work I'm doing in Digital Preservation.

Wednesday, February 9, 2022

EE380 Talk

I was asked at short notice to fill in for a speaker in Stanford's EE380 course who had to cancel. Below the fold is a hastily updated version of a talk from last December.

[Slide 1: Title]
I apologize if this talk is a bit rough. Dennis mailed me yesterday morning asking if I could speak, so I updated a talk I gave in December to an Institutional Investor conference. You don't need to take notes; the text of this talk with links to the sources and much additional material will be on blog.dshr.org. I'm aiming to talk for 30 minutes and be controversial enough to spark a discussion, so please hold questions.

I'm David Rosenthal. I worked with James Gosling on CMU's Andrew project in the early 80s. I was a DE with him at Sun later in the 80s working on window systems including X, and file systems. I quit to be employee #4 at Nvidia where Curtis Priem and I did the basic I/O architecture, then was an early employee at Vitria, the second company of founders of Tibco. Before I start talking about cryptocurrencies, I should stress that I hold no long or short positions in cryptocurrencies, their derivatives or related companies; I am long Nvidia. Unlike most people discussing them, I am not "talking my book".

Cryptocurrencies' roots lie deep in the libertarian culture of Silicon Valley and the cypherpunks. Libertarianism's attraction is based on ignoring externalities, and cryptocurrencies are no exception.

[Slide 2: Externalities]
Bitcoin is notorious for consuming as much electricity as the Netherlands, but there are around 10,000 other cryptocurrencies, most using similar infrastructure and thus also in aggregate consuming unsustainable amounts of electricity. Bitcoin alone generates as much e-waste as the Netherlands, cryptocurrencies suffer an epidemic of pump-and-dump schemes and wash trading, they enable a $5.2B/year ransomware industry, they have disrupted supply chains for GPUs, hard disks, SSDs and other chips, they have made it impossible for web services to offer free tiers, and they are responsible for a massive crime wave including fraud, theft, tax evasion, funding of rogue states such as North Korea, drug smuggling, and even as documented by Jameson Lopp's list of physical attacks, armed robbery, kidnapping, torture and murder.

[Slide 3: Alecus]
The attempt to force El Salvador's population to use cryptocurrency is a fiasco. They offer no significant social benefit beyond speculation; Igor Makarov and Antoinette Schoar write:

Alecus, *El Diario de Hoy*

> 90% of transaction volume on the Bitcoin blockchain is not tied to economically meaningful activities but is the byproduct of the Bitcoin protocol design as well as the preference of many participants for anonymity. ...
> exchanges play a central role in the Bitcoin system. They explain 75% of real Bitcoin volume
> ...
> Our results do not support the idea that the high valuation of

Blog Rules

DSHR

DSHR in ANWR

Recent Comments

David.
Some reactions to this talk on Twitter here, I love that it rated an "Old man yells at Bitcoin".

David.
jerdavis, I see you rely on sources who are "talking their book". I prefer not to.

David.
In 'Full Self-Driving' clips show owners of Teslas fighting for control, and experts see deep flaws, Faiz Siddiqui and R…More

jerdavis
Sir, right off the top you lead with some dubious info.The ewaste paper is generally discredited because of incorrect li…More

David.
The regulators' unhappiness with Tesla's casual attitude to safety continues, as Richard Currie reports in '…More

Full comments

cryptocurrencies is based on the demand from illegal transactions. Instead, they suggest that the majority of Bitcoin transactions is linked to speculation.

[Slide 4: "Transaction" Rate]
Bitcoin is only processing around 27K "economically meaningful" transactions/day. And 75% of those are transactions between exchanges, so only 2.5% of the "transactions" are real blockchain-based transfers involving individuals. That's less than 5 per minute.

Source

Nakamoto's motivation for Bitcoin was distrust of institutions, especially central banks. When it launched in the early stage of the Global Financial Crisis, this had resonance. The key to a system that involves less trust is decentralization.

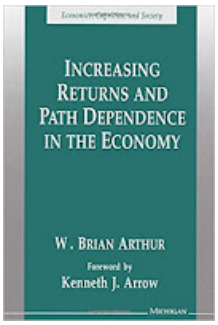
[Slide 5: Resilience]
Why do suspension bridges have stranded cables not solid rods? The major reason is that solid rods would fail suddenly and catastrophically, whereas stranded cables fail slowly and make alarming noises while they do. We build software systems out of solid rods; they fail abruptly and completely. Most are designed to perform their tasks as fast as possible, so that when they are compromised, they perform the attacker's tasks as fast as possible. Changing this, making systems that are resilient, ductile like copper not brittle like glass, is an extraordinarily difficult problem in software engineering. Paul Vixie pointed out that rate limits are an essential part of the solution.


Source

I got interested in it when, burnt out after three startups all of which IPO-ed, I started work at the Stanford Library on the problem of keeping digital information safe for the long term. This work won my Stanford CS co-authors (Petros Maniatis, Mema Roussopolous, TJ Giuli and Prof. Mary Baker) and I a "Best Paper" award at the 2003 SOSP for a decentralized consensus system using Proof-of-Work. When, five years later, Satoshi Nakamoto published the Bitcoin protocol, a cryptocurrency based on a decentralized consensus mechanism using Proof-of-Work, I was naturally interested in how it turned out.

Decentralization is a necessary but insufficient requirement for system resilience. Centralized systems have a single locus of control. Subvert it, and the system is at your mercy. It only took six years for Bitcoin to fail Nakamto's goal of decentralization, with one mining pool controlling more than half the mining power. In the seven years since no more than five pools have always controlled a majority of the mining power.

[Slide 6: Economies of Scale]
In 2014 I wrote *Economies of Scale in Peer-to-Peer Networks*, explaining the economic cause of this failure. Briefly, this is an example of the phenomenon described by W. Brian Arthur in 1994's *Increasing returns and path dependence in the economy*. Information technologies have strong economies of scale, so the larger the miner the lower their costs, and thus the greater their profit, and thus the greater their market share.



Source

"Blockchain" is unfortunately a term used to describe two completely different technologies, which have in common only that they both use a Merkle Tree data structure. *Permissioned* blockchains have a central authority controlling which network nodes can add blocks to the chain, and are thus not decentralized, whereas *permissionless* blockchains such as Bitcoin's do not; this difference is fundamental:

- Permissioned blockchains can use well-established and relatively efficient techniques such as Byzantine Fault Tolerance, and thus don't have significant carbon footprints. These techniques ensure that each node in the network has performed the same computation on the same data to arrive at the *same* state for the next block in the chain. This is a *consensus* mechanism.

Blog Archive

▼ 2022 (10)
▼ February (3)
EE380 Talk
USA Number 1!
List And Dump Schemes
► January (7)
► 2021 (62)
► 2020 (55)
► 2019 (66)
► 2018 (96)
► 2017 (82)
► 2016 (89)
► 2015 (75)
► 2014 (68)
► 2013 (67)
► 2012 (43)
► 2011 (40)
► 2010 (17)
► 2009 (8)
► 2008 (8)
► 2007 (14)

- In principle each node in a permissionless blockchain's network can perform a different computation on different data to arrive at a *different* state for the next block in the chain. Which of these blocks ends up in the chain is determined by a randomized, biased *election* mechanism. For example, in Proof-of-Work blockchains such as Bitcoin's a node wins election by being the first to solve a puzzle. The length of time it takes to solve the puzzle is random, but the probability of being first is biased, it is proportional to the compute power the node uses. Initially, because of network latencies, nodes may disagree as to the next block in the chain, but eventually it will become clear which block gained the most acceptance among the nodes. This is why a Bitcoin transaction should not be regarded as final until it is six blocks from the head.

[Slide 7: Blockchain Patent Filed 1990]
Discussing "blockchains" and their externalities without specifying permissionless or permissioned is meaningless, they are completely different technologies. One is 30 years old, the other is 13 years old.


United States Patent [19]
Haber et al.
[11] Patent Number: 5,136,647
[45] Date of Patent: Aug. 4, 1992
[54] METHOD FOR SECURE TIME-STAMPING OF DIGITAL DOCUMENTS
ABSTRACT
OTHER PUBLICATIONS
Source

Because there is no central authority controlling who can participate, decentralized consensus systems must defend against Sybil attacks, in which the attacker creates a majority of seemingly independent participants which are secretly under his control. The defense is to ensure that the reward for a successful Sybil attack is less than the cost of mounting it. Thus participation in a permissionless blockchain must be expensive, so miners must be reimbursed for their costly efforts. There is no central authority capable of collecting funds from users and distributing them to the miners in proportion to these efforts. Thus miners' reimbursement must be generated organically by the blockchain itself; a permissionless blockchain needs a cryptocurrency to be secure.

Because miners' opex and capex costs cannot be paid in the blockchain's cryptocurrency, exchanges are required to enable the rewards for mining to be converted into fiat currency to pay these costs. Someone needs to be on the other side of these sell orders. The *only* reason to be on the buy side of these orders is the belief that "number go up". Thus the exchanges need to attract speculators in order to perform their function.

Thus a permissionless blockchain *requires* a cryptocurrency to function, and this cryptocurrency *requires* speculation to function.

Why are economies of scale a fundamental problem for decentralized systems? Participation must be expensive, and so will be subject to economies of scale. They will drive the system to centralize. So the expenditure in attempting to ensure that the system is decentralized is a futile waste.

Most cryptocurrencies impose these costs, as our earlier system did, using Proof-of-Work. It was a brilliant idea when Cynthia Dwork and Moni Naor originated it in 1992, being both simple and effective. But when it is required to make participation expensive enough for a trillion-dollar cryptocurrency it has an unsustainable carbon footprint.

[Slide 8: Bitcoin Energy Consumption]
The leading source for estimating Bitcoin's electricity consumption is the Cambridge Bitcoin Energy Consumption Index, whose current central estimate is 117TWh/year.

Source

Adjusting Christian Stoll *et al*'s 2018 estimate of Bitcoin's carbon footprint to the current CBECI estimate gives a range of about 50.4 to 125.7 MtCO2/yr for Bitcoin's opex emissions, or between Portugal and Myanmar. Unfortunately, this is likely to be a considerable underestimate. *Bitcoin's growing e-waste problem* by Alex de Vries and Christian Stoll concludes that:

> Bitcoin's annual e-waste generation adds up to 30.7 metric kilotons as of May 2021. This level is comparable to the small IT equipment waste produced by a country such as the Netherlands.

That's an average of one whole MacBook Air of e-waste *per "economically meaningful" transaction*.

[Slide 9: Facebook & Google Carbon Footprints]
The reason for this extraordinary waste is that the profitability of mining depends on the energy consumed per hash, and the rapid development of mining ASICs means that they rapidly become uncompetitive. de Vries and Stoll estimate that the average service life is less than 16 months. This mountain of e-waste contains embedded carbon emissions from its manufacture, transport and disposal. These graphs show that for Facebook and Google data centers, capex emissions are at least as great as the opex emissions[1].

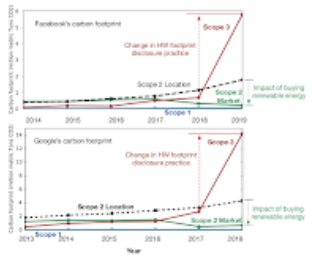


Fig. 11. Carbon footprint of Facebook and Google (two large data center operators). As data centers increasingly rely on renewable energy, carbon emissions originate more from Scope 3, or supply-chain emissions (e.g., hardware manufacturing and construction).

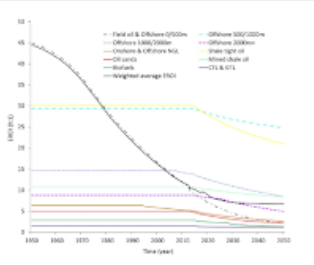
Source

Cryptocurrencies assume that society is committed to this waste of energy and hardware *forever*. Their response is frantic greenwashing, such as claiming that because Bitcoin mining allows an obsolete, uncompetitive coal-burning plant near St. Louis to *continue burning coal* it is somehow good for the environment[2].

But, they argue, mining can use renewable energy. First, at present it doesn't. For example, Luxxfolio implemented their commitment to 100% renewable energy by buying 15 megawatts of coal-fired power from the Navajo Nation!.

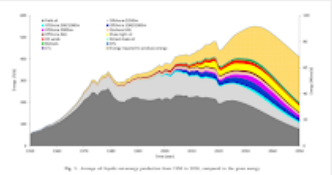
Second, even if it were true that cryptocurrencies ran on renewable power, the idea that it is OK for speculation to waste vast amounts of renewable power assumes that doing so doesn't compete with more socially valuable uses for renewables, or indeed for power in general.

[Slide 10: Energy Return on Investment]
Right now the world is short of power; one major reason that China banned cryptocurrency mining was that they needed their limited supplies of power to keep factories running and homes warm. Shortage of energy isn't a short-term problem. This graph is from *Peak oil and the low-carbon energy transition: A net-energy perspective* by Louis Delannoy *et al* showing that as the easiest deposits are exploited first, the Energy Return On Investment, measuring the fraction of the total energy extracted delivered to consumers, decreases.



Delannoy *et al* Fig 2

[Slide 11: Oil Energy Gross vs. Net]



Delannoy *et al* Fig 1

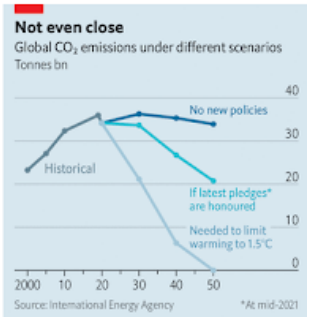
Delannoy *et al*'s Figure 1 shows the gross and net oil energy history and projects it to 2050. The gross energy, and thus the carbon emission, peaks around 2035, but because the energy used in extraction (the top yellow band) increases rapidly, the net energy peaks in about 5 years.

[Slide 12: CO2 Emission Trajectories]
This is a problem for two reasons. If society is to survive:

- Carbon emissions need to start decreasing *now*, not in a decade and a half.
- Renewables need to be deployed very rapidly.

Deploying renewables consumes energy, which is paid back during their initial operation. Thus the

current transition to renewable power consumes energy, reducing that available for other uses[3]. The world cannot afford to waste a Netherlands' worth of energy on speculation that could instead be deploying renewables.



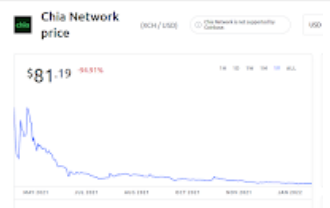
Source

If cryptocurrency speculation is to continue, it needs to vastly reduce its carbon footprint by eliminating Proof-of-Work. The two major candidates are Proof-of-Space-and-Time and Proof-of-Stake.

Proof-of-Space-and-Time attempts to make participation expensive by wasting storage instead of computation. The highest-profile such effort is Bram Cohen's *Chia*, funded by Andreesen Horowitz, the "Softbank of crypto". Chia's "space farmers" create and store "plots" consisting of large amounts of otherwise useless data.

[Slide 13: Chia]

The software was ingenious, but the design suffered from naiveté about storage media and markets. When it launched in May, gullible farmers rushed to buy hard disks and SSDs. By July, the capital tied up in farming hardware was around *six times* the market cap of the Chia coin. Chia's CEO described the result:



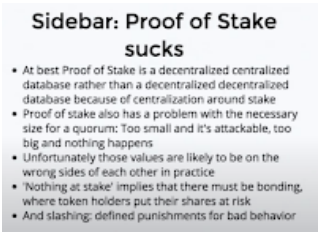
Source

> "we've kind of destroyed the short-term supply chain"

Disk vendors were forced to explain that Chia farming voided the media's warranty. Just as with GPUs, the used market was flooded with burnt-out storage. Chia's coin initially traded at $1934 before dropping more than 90% — last I looked it was $81. I expect A16Z made money, but everyone else had to deal with the costs. Chia doesn't use much electricity, more to do with failure than with the technology, but does have a major e-waste problem.

[Slide 14: Proof of Stake Sucks]

The costs that Proof-of-Stake imposes to make participation expensive are the risk of loss and the foregone liquidity of the "stake", an escrowed amount of the cryptocurrency itself. This has two philosophical problems:



Bram Cohen's opinion

- It isn't just that the Gini coefficients of cryptocurrencies are extremely high[4], but that Proof-of-Stake makes this a self-reinforcing problem. Because the rewards for mining new blocks, and the fees for including transactions in blocks, flow to the HODL-ers in proportion to their HODL-ings, whatever Gini coefficient the systems starts out with will always increase. Proof-of-Stake isn't effective at decentralization.
- Cryptocurrency whales are believers in "number go up". The eventual progress of their coin "to the moon!" means that the temporary costs of staking are irrelevant.

There are also a host of severe technical problems. The accomplished Ethereum team have been making a praiseworthy effort to overcome them for more than 7 years and are still more than a year away from being able to migrate off Proof-of-Work.

[Slide 15:Centralization Risk]

> Yulin Cheng wrote:
>
> > According to the list of accounts powered up on March. 2, the three exchanges collectively put in over 42 million STEEM Power (SP).
> >
> > With an overwhelming amount of stake, the Steemit team was

> then able to unilaterally implement hard fork 22.5 to regain their stake and vote out all top 20 community witnesses – server operators responsible for block production – using account @dev365 as a proxy. In the current list of Steem witnesses, Steemit and TRON's own witnesses took up the first 20 slots.

Vitalik Buterin pointed out that lack of decentralization was a security risk in 2017, and this was amply borne out last year when Justin Sun conspired with three exchanges, staking their customers coins to take over the Steem Proof-of-Stake blockchain. Pushing back against the economic forces centralizing these systems is extremely difficult.

[Slide 16: Top 2 ETH Pools = 53.9%]
The advantage of permissionless over permissioned blockchains is claimed to be decentralization. How has that worked out in practice?

Source

As has been true for the last seven years, no more than five mining pools control the majority of the Bitcoin mining power and last November two pools controlled the majority of Ethereum mining. Makarov and Schoar write:

> Six out of the largest mining pools are registered in China and have strong ties to Bitmain Techonologies, which is the largest producer of Bitcoin mining hardware,

[Slide 17: Centralized Mining]

Makarov and Schoar write:

> Bitcoin mining capacity is highly concentrated and has been for the last five years. The top 10% of miners control 90% and just 0.1% (about 50 miners) control close to 50% of mining capacity. Furthermore, this concentration of mining capacity is counter cyclical and varies with the Bitcoin price. It decreases following sharp increases in the Bitcoin price and increases in periods when the price drops ... the risk of a 51% attack increases in times when the Bitcoin price drops precipitously or following the halving events.

It isn't just the mining pools that are centralized. The top 10% of miners control 90% and just 0.1% (about 50 miners) control close to 50% of mining capacity. This centralization doesn't just increase the system's technical risk, but also its legal risk. The reason is that in almost all cryptocurrencies a transaction wishing to be confirmed is submitted to a public "mempool" of pending transactions. The mining pools choose transactions from there to include in the blocks they attempt to mine. This, as Nicholas Weaver points out, means that mining pools are providing money transmission services under US law:
[Slide 18: 31 CFR § 1010.100]

> The term "money transmission services" means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.

Thus, in the US, they are required to follow the Anti-Money Laundering/Know Your Customer (AML/KYC) rules as enforced by the Financial Crimes Enforcement Network (FinCEN)[6]. The only pool to try following them:

> stopped doing this because the larger Bitcoin community objects to the idea of attempting to restrict Bitcoin to legal uses!

As Adem Efe Gencer *et al* pointed out:

> a Byzantine quorum system of size 20 could achieve better decentralization than proof-of-work mining at a much lower resource cost.

Thus the only reason for the massive carbon footprint of Proof-of-Work and the complexity and risk of the alternatives is to maintain the illusion of decentralization. Alas, it is unlikely that any alternative defense against Sybil attacks will be widely enough adopted to mitigate Proof-of-Work's carbon emissions.

[Slide 19: Immutability]

Source

Immutability is one of the two things that make the cryptocurrency crime wave so effective. These systems are brittle, make a single momentary mistake and your assets are irretrievable.

Immutability sounds like a great idea when everything is going to plan, but in the real world mistakes are inevitable. Lets take a few recent examples — the $23M fee Bitfinex paid for a $100K transaction, or the $19M oopsie at Indexed Finance, or the $31M oopsie at MonoX, or the $90M oopsie at Compound and the subsequent $67M oopsie, all of which left the perpetrators pleading with the benficiaries to return the loot. And in Compound's case threatening its customers with the ultimate crypto punishment, reporting them to the IRS. $12B in DeFi thefts so far, or about 5% of all the funds[7].

[Slide 20: Trammell Hudson]

Source

Vulnerabilities are equally inevitable, as we see with the $38M, $19M and $130M hacks of Cream Finance last year, the $115M hack of BadgerDAO, the $196M hack of BitMart, the recent $323M hack of Wormhole, and of course the $600M hack of Poly Network.

Because Ethereum and similar cryptocurrencies are programming environments, their attack surface is much larger than Bitcoin's. Now that DeFi and NFT protocols are implemented as "smart contracts" in these environments, the attack surface has expanded much further. One example is the rash of hacks involving hijacks of the Discord servers of the communities surrounding them to lure victims into autheticating their wallets to malign "smart contracts". Another is the flood of "rug-pulls" buried in the "smart contracts" implementing NFTs.

[Slide 21: Jacob Silverman]

Jacob Silverman
@SilvermanJacob

Imagine if big banks were getting hacked for tens or hundreds of millions of $$ each week but also nothing was insured, there were no systems in place to mitigate fallout, and half of the hacks were inside jobs. That's basically DeFi.

5:15 PM · Feb 2, 2022

762 Reply Share

Read 21 replies

Yet another is described in Dan Goodin's *How $323M in crypto was stolen from a blockchain bridge called Wormhole*. Because there are many competing blockchains, bridges exist to provide liquidity between them. Last month Vitalik Buterin provided a detailed explanation of why they are a fundamental security problem. A "smart contract" called a guardian locks up coins on one blockchain and unlocks the same number on

another, but in this case the guardian failed to properly validate signatures.
[Slide 22: Wormhole Vulnerability]

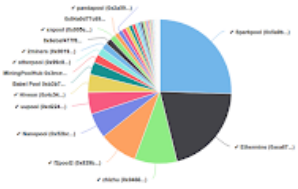
> **samczsun** @samczsun · Feb 2, 2022
> Replying to @samczsun
> Once they had the fake `SignatureSet`, it was trivial to use it to generate a valid VAA and trigger an unauthorized mint to their own account. The rest is history.
>
> **samczsun**
> @samczsun
>
> tl;dr - Wormhole didn't properly validate all input accounts, which allowed the attacker to spoof guardian signatures and mint 120,000 ETH on Solana, of which they bridged 93,750 back to Ethereum.
>
> 5:16 PM · Feb 2, 2022
>
> 1.4K Reply Share
>
> **Read 68 replies**

Three days later a bug in another bridge was exploited for $4.3M.

The centralization of Ethereum's mining pools and exchanges enabled Poly Network to persuade them to blacklist the addresses involved. This made it very difficult for the miscreant to escape with the loot, much of which was returned. But it also vividly demonstrated that in most blockchains it is the mining pools that decide which transactions make it into a block, and are thus executed. The small number of dominant mining pools can effectively prevent addresses from transacting, and can prioritize transactions from favored addresses. They can also allow transactions to avoid the public mempool, to prevent them being front-run by bots. This turned out to be useful when a small group of white hats discovered a vulnerability in a smart contract holding $9.6M.

The key point of *Escaping the Dark Forest*, Samczsun's account of their night's work, is that, after the group spotted the vulnerability and built a transaction to rescue the funds, they could not put the rescue transaction in the public mempool because it would have been front-run by a bot. They had to find a miner who would put the transaction in a block *without* it appearing in the mempool. In other words, their transaction needed a dark pool. And they had to trust the cooperative miner not to front-run it.

[Slide 23: Ether Mining Pools 11/02/20]
Ethereum is, fortunately, very far from decentralized, being centralized around a small number of large pools. Thus, the group needed a trusted pool not an individual miner. At the time, the three largest pools mined more than half the blocks between them, so only three calls would have been needed to have a very good chance that the transaction would appear in one of the next few blocks.



Ether miners 11/2/20

Most activity in "trustless" cryptocurrencies actually uses trusted third parties, exchanges, that are layered above the blockchain itself. These use conventional Web-based identities and provide another layer of centralization. Binance, the dominant exchange, does two out of three derivative transactions and half of all spot transactions. Adam Levitin points out that customers are *unsecured creditors* of exchanges. Exchanges are routinely compromised; in most cases immutability means the pilfered funds are not recovered.

But, more fundamentally, the entire cryptocurrency ecosystem depends upon a trusted third party, Tether, which acts as a central bank issuing the "stablecoins" that cryptocurrencies are priced against and traded in[8]. This is despite the fact that Tether is known to be untrustworthy, having consistently lied about its reserves.

[Slide 24: Anonymity]

Makarov and Schoar write[9]:

> First, non-KYC entities serve as a gateway for money laundering and other gray activities.
> ...
> Second, even if KYC entities were restricted to deal exclusively with other KYC entities, preventing inflows of tainted funds would still be nearly impossible, unless one was willing to put severe restrictions on who can transact with whom
> ...
> Finally, notice that while transacting in cash and storing cash involve substantial costs and operational risks, transacting in cryptocurrencies and storing them are essentially costless (apart from fluctuation in value).

The other main enabler of the cryptocurrency crime spree is the prospect of transactions that aren't merely immutable but are also anonymous. Anonymity for small transactions is important, but for large transactions it provides the infrastructure for major crime. In the physical world cash is anonymous, but it has the valuable property that the cost and difficulty of transacting increase strongly with size. KYC/AML and other regulations leverage this. Cryptocurrencies lack this property. The ease with which cryptocurrency can be transferred between institutions that do, and do not, observe the KYC/AML regulations means that absent robust action by the US, the KYC/AML regime is doomed.

[Slide 25: The Coming Ransomware Storm]

Stephen Diehl writes in *The Oncoming Ransomware Storm*:

> Go to your local bank branch and try to wire transfer $200,000 to an anonymous stranger in Russia and see how that works out. Modern ransomware could not exist without Bitcoin, it has poured gasoline on a fire we may not be able to put out.
>
> When you create a loophole channel (however flawed) for parties to engage in illicit financing of anonymous entities beyond the control of law enforcement, it turns out a lot of shady businesses models that are otherwise prevented move from being impractical and risky to perversely incentivized. Ransomware is now very lucrative to the point where there is a whole secondary market of vendors selling Ransomware as a Service picks and shovels to the criminals.

The most serious crime enabled by anonymity is ransomware, which is regularly crippling essential infrastructure such as oil pipelines and hospital systems, to say nothing of the losses to business large and small. This business is estimated to gross $5.2B/year and is growing rapidly, aided by a network of specialist service providers. This is just the ransom payments, the actual externalities include the much larger costs of recovering from the attacks.

There are cryptocurrencies that provide almost complete anonymity using sophisticated cryptography[10]. For example Monero:

> Observers cannot decipher addresses trading monero, transaction amounts, address balances, or transaction histories.

Bitcoin and similar cryptocurrencies are *pseudonymous* not anonymous. Anyone can create and use an essentially unlimited number of pseudonyms (addresses), but transactions and balances using them are public. A newly minted pseudonym cannot be deanonymized, but as it becomes enmeshed in the public web of transactions maintaining anonymity takes more operational security than most users can manage.

Users are aware of the risk that their transactions can be traced, so many engage in wash transactions between addresses they control, and use mixers and tumblers to mingle their coins with those of other miscreants. Because it is almost impossible to actually buy legal goods with Bitcoin, at some point a HODL-er needs to use an exchange to obtain fiat currency[11]. This risks having their identity connected into the web of transactions on the blockchain. Makarov and Schoar conclude:

> 90% of transaction volume on the Bitcoin blockchain is not tied to economically meaningful activities but is the byproduct of the Bitcoin protocol design as well as the preference of many participants for anonymity.

In other words, 90% of Bitcoin's carbon footprint is used in a partially successful attempt to compensate for its deficient anonymity.

Because there are existing alternatives that provide greatly increased anonymity, attempts to mitigate the externalities of pseudonoymous cryptocurrencies are likely to be self-defeating. As the ransomware industry shows, users will migrate to these alternatives, reducing the effectiveness of chain analysis.

[Slide 26: Conclusions]
Although the techniques used to implement decentralization are effective in theory, at scale emergent economic effects render them ineffective. Despite this, decentralization is fundamental to the cryptocurrency ideology, making mitigation of its externalities effectively impossible. And attempts to mitigate the externalities of pseudonymous cryptocurrencies are lijkely to be self-defeating. We can conclude that:

1. Permissioned blockchains do not need a cryptocurrency to defend against Sybil attacks, and thus do not have significant externalities.
2. Permissionless blockchains require a cryptocurrency, and thus necessarily impose all the externalities I have described except the carbon footprint.
3. If successful, permissionless blockchains using Proof-of-Work, or any other way to waste a real resource as a Sybil defense, have unacceptable carbon footprints.
4. Whatever Sybil defense they use, economics forces successful permissionless blockchains to centralize; there is no justification for wasting resources in a doomed attempt at decentralization.

Don't get me wrong. I am not a fan of centralization. I started building a decentralized, permissionless system almost a quarter-century ago. It would be wonderful if we could figure out how to build a Web that would resist centralization. But all the technical and financial cleverness that's been poured into cryptocurrencies hasn't succeeded in doing that. Why? It is because *It Isn't About The Technology*.

I'm a big believer in Bill Joy's Law of Startups, "success is inversely proportional to the amount of money you have". For $2.5M we got Nvidia to working silicon that was revolutionary in two different respects. Right now, there is way too much money. If a system is to be decentralized, it has to have a low barrier to entry. If it has a low barrier to entry, competition will ensure it has low margins. Low margin businesses don't attract venture capital. VCs are pouring money into cryptocurrency and "web3" companies. This money is not going to build systems with low barriers to entry and thus low margins. Thus the systems that will result from this flood of money will not be decentralized, no matter what the sales pitch says.

Despite all the cleverness and hype, the technology just isn't that good. It is both extraordinarily inefficient, and extraordinarily insecure. Nicholas Weaver points out that the "Ethereum computer" is 1/5000 as powerful as a Raspbery Pi. and that for the cost of 1 second of its use you can buy nearly 60 Raspberry Pis. Moxie Marlinspike points out that an NFT is a link to a file of metadata that links to the image it purports to represent, so neither is guaranteed to exist or be valid. You have only to glance at Molly White's *Web3 is going just great* timeline wonder why anyone thinks this "wretched hive of scum and villainy" should be the future of the Web.

I hope I've said enough to start some discussion. I think there are three basic lines of argument:

- That the externalities I describe don't exist. You'll have a hard time proving that the waste of electricity and hardware, and the crime wave, are imaginary.

- That although the externalities do exist, the benefits of decentralization outweigh them. The problem here is that since the systems are not actually decentralized, we get the externalities but don't get the benefits.
- That although the externalities do exist, and the systems aren't dencentralized, they're making so much money that we shouldn't worry. The problem here is that the amount of actual money you can get out of a cryptocurrency equals the amount of actual money that has been put in, minus the actual costs of mining. So the big picture is that although there may be winners, in aggregate the system loses money.

End Notes

1. Ethereum mining adds another 23.7TWh/yr (16.5 to 32 range) for about 6.9MtCO2/yr, according to Kyle McDonald.

   Doubling the carbon footprint to account for embedded emissions would put Bitcoin between Zimbabwe and Thailand. It would put Ethereum between Uruguay and Yemen, but it is likely that this would be an over-estimate, since GPUs are likely to have a somewhat longer economic life.

   Note the hockey-stick on these graphs. I wrote:

   > In 2017 Facebook and Google changed their capex footprint disclosure practice, resulting in an increase of 7x for Google and 12x for Facebook. It is safe to assume that neither would have done this had they believed the new practice greatly over-estimated the footprint.

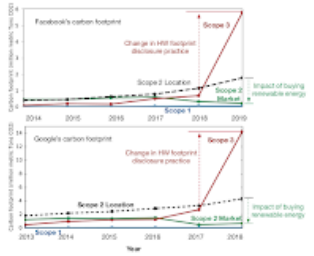
   

   Fig. 11. Carbon footprint of Facebook and Google (two large data center operators). As data centers increasingly rely on renewable energy, carbon emissions originate more from Scope 3, or supply-chain emissions (e.g., hardware manufacturing and construction).

   Source

   If Google and Facebook are correctly measuring their capex emissions, and if they are representative of miners' capex emssions, cryptocurrencies' carbon footprints are vastly more than double that from their opex emssions alone.
2. And lobbying. See, for example, the way the climate aspects of "Build Back Better" were crippled to facilitate the plant that is the sole customer of the company that pays Joe Manchin $500K/year transitioning to burning Manchin's waste coal to mine cryptocurrency.
3. Sweden's regulators make this point in an open letter to the EU:

   > Sweden needs the renewable energy targeted by crypto-asset producers for the climate transition of our essential services, and increased use by miners threatens our ability to meet the Paris Agreement. Energy-intensive mining of crypto-assets should therefore be prohibited. This is the conclusion of the director generals of both the Swedish Financial Supervisory Authority and the Swedish Environmental Protection Agency.

   And the Norwegians agree.
4. Makarov and Schoar write:

   > We show that the balances held at intermediaries have been steadily increasing since 2014. By the end of 2020 it is equal to 5.5 million bitcoins, roughly one-third of Bitcoin in circulation. In contrast, individual investors collectively control 8.5 million bitcoins by the end of 2020. The individual holdings are still highly concentrated: the top 1000 investors control about 3 million BTC and the top 10,000 investors own around 5 million bitcoins.

5. Five years after Ethereum Classic became the remainder of the vulnerable currency, the result was:

   > from the beginning of March to the beginning of May, the value of Ethereum Classic had shot up by over 1,000 percent. It jumped from about $12 a token to over $130.

6. David Gerard provides a comprehensive overview of the latest "regulatory clarity" on cryptocurrencies from the international and US government agencies:
    - The Financial Action Task Force issued *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*. Gerard writes

        > The October 2021 revision is to clarify definitions, give guidance on stablecoins, note the issues of peer-to-peer transactions, and clarify the travel rule, which requires VASPs to collect and pass on information about their customers.
        >
        > VASPs include crypto exchanges, crypto transfer services, crypto custody and financial services around crypto asset issuance (e.g., ICOs). VASPs must do full Know-Your-Customer (KYC), just like any other financial institution.

      As regard peer-to-peer transactions, Gerard writes:

        > Jurisdictions should assess the local risks from peer-to-peer transactions, and possibly adopt optional provisions, such as restricting direct deposit of cryptos with VASPs (paragraphs 105 and 106) — Germany and Switzerland have already considered such rules.

    - The US Office of Foreign Assets Control's *Sanctions Compliance Guidance for the Virtual Currency Industry* explains that:

        > Members of the virtual currency industry are responsible for ensuring that they do not engage, directly or indirectly, in transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade- or investment-related transactions.

      In particular, US miners are required to blacklist wallets suspected of being owned by sanctioned entities. Gerard writes:

        > Sanctions are strict liability — you can be held liable even if you didn't know you were dealing with a sanctioned entity. Penalties can be severe, but OFAC recommends voluntary self-disclosure in case of errors, and this can mitigate penalties. You will be expected to correct the root cause of the violations.

    - The US Financial Crimes Enforcement Network issued *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*. Gerard writes:

        > Insurers and and "digital forensic and incident response" companies have been getting more directly involved in ransomware payments — even paying out the ransoms. FinCEN expects such companies to: (a) register as money transmitters; (b) stop doing this.
        >
        > A lot of ransomware gangs are sanctioned groups or individuals. Payments to them are sanctions violations.

      The Federal Reserve, the FDIC and the OCC have joined the party with a *Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps*. They:

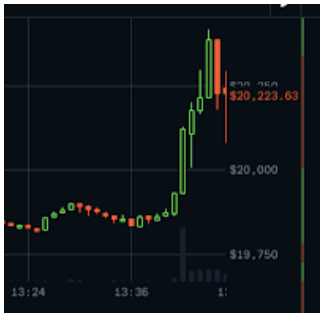
        > plan to provide greater clarity on whether certain activities related to crypto-assets conducted by banking organisations are legally permissible, and expectations for safety and soundness, consumer protection, and compliance with existing laws and regulations

7. In *Really stupid "smart contract" bug let hackers steal $31 million in digital coin*, Dan Goodin reports that:

> blockchain-analysis company Elliptic said so-called DeFi protocols have lost $12 billion to date due to theft and fraud. Losses in the first roughly 10 months of this year reached $10.5 billion, up from $1.5 billion in 2020.

That is ~5% of the $237B locked up in DeFi.

8. But the only significant social benefit of cryptocurrencies is rampant speculation, mostly in an enormous Bitcoin futures market using up to 125x leverage, based on a Bitcoin-Tether market about one-tenth the size, based on a Bitcoin-USD market about one-tenth the size again. The Bitcoin-Tether market is highly concentrated, easily manipulated and rife with pump-and-dump schemes.



A New Wolf in Town? Pump-and-Dump Manipulation in Cryptocurrency Markets by Anirudh Dhawan and Tālis J. Putniņš finds:

> Combining hand-collected data with audited data from a pump-and-dump aggregator, we identify as many as 355 cases of pump-and-dump manipulation within a period of six months on two cryptocurrency exchanges. Up to 23 million individuals are involved in these manipulations. We estimate that the 355 pumps in our sample are associated with approximately $350 million of trading on the manipulation days, and that manipulators extract profits of approximately $6 million from other participants. In all, 197 distinct cryptocurrencies or "coins" are manipulated, which implies that approximately 15% of all coins in our sample of exchanges are targeted by manipulators at least once in the six-month period. There are, on average, two pumps per day. This rate of manipulation is considerably higher than pump-and-dump manipulation in stock markets in recent decades.

See also this post on the strange fact that:

> The futures curve for Bitcoin has been permanently upward sloping in Contango pretty much since inception, back in 2017 meaning that the price of the future asset is higher than the spot price of the asset for pretty much 4 years
> ...
> The implication that this arbitrage opportunity persistently exists and is not hammered by investors until it closes, is that there is some form of market dislocation or systemic credit risk that cannot be properly quantified or hedged.

And on Celsius' offer of 17% interest on BTC loans, which clearly indicates a high degree of risk. Note that:

> Yaron Shalem, the chief financial officer of cryptocurrency lending platform Celsius, was one of the seven people arrested in Tel Aviv this month in connection with Israeli crypto mogul Moshe Hogeg

9. Transaction fees make Makarov and Schoar's claim that "transacting in cryptocurrencies and storing them are essentially costless" false. The demand for transactions is variable, but the supply is fixed. Pending transactions bid their fees in a blind auction for inclusion in a block. The result is that when no-one wants to transact fees are low and when everyone does they spike enormously.

The graph shows that as the Bitcoin "price" spiked to $63K in April the frenzy drove the *average* fee per transaction over $60. User's lack of understanding of transaction fees is illustrated by Jordan Pearson and Jason

Koebler's *'Buy the Constitution' Aftermath: Everyone Very Mad, Confused, Losing Lots of Money, Fighting, Crying, Etc.*:


BTC transaction fees

> The community of crypto investors who tried and failed to buy a copy of the U.S. Constitution last week has descended into chaos as people are realizing today that roughly half of the donors will have the majority of their investment wiped out by cryptocurrency fees.

Apparently, fees averaged $50/transaction, and the $40M raised paid about $1M in fees. That is 2.5%, very similar to the "extortionate" fees charged by credit card companies that cryptocurrency enthusiasts routinely decry.

Vitalik Buterin has a proposal that attempts to paper over the fundamental problem of fixed supply and variable demand, as Ruholamin Haqshanas reports in *Vitalik Buterin Proposes New EIP to Tackle Ethereum's Sky-High Gas Fees*:

Source

> Vitalik Buterin has put forward a new Ethereum Improvement Proposal (EIP) that aims to tackle the network's gas fee problems by adding a limit on the total transaction calldata, which would, in turn, should reduce transaction gas cost.
>
> Since Ethereum can only process 15 transactions per second, gas fees tend to spike at times of network congestion. On November 9, the average transaction network fee reached USD 62 per transaction. As of now, Ethereum transactions cost around USD 44,

10. With the Taproot soft fork, explained in *WHY YOU SHOULD CARE ABOUT TAPROOT, THE NEXT MAJOR BITCOIN UPGRADE*, Bitcoin is making transactions slightly more difficult to trace, but still not offering the anonymity of Monero:

> The Taproot upgrade improves this logic by introducing Merklelized Abstract Syntax Trees (MAST), a structure that ultimately allows Bitcoin to achieve the goal of only revealing the contract's specific spending condition that was used.
>
> There are two main possibilities for complex Taproot spending: a consensual, mutually-agreed condition; or a fallback, specific condition. For instance, if a multisignature address owned by multiple people wants to spend some funds programmatically, they could set up one spending condition in which all of them agree to spend the funds or fallback states in case they can't reach a consensus.
>
> If the condition everyone agrees on is used, Taproot allows it to be turned into a single signature. Therefore, the Bitcoin network wouldn't even know there was a contract being used in the first place, significantly increasing the privacy of all of the owners of the multisignature address.
>
> However, if a mutual consensus isn't reached and one party spends the funds using any of the fallback methods, Taproot only reveals that specific method. As the introduction of P2SH increased the receiver's privacy by making all outputs look identical — just a hash — Taproot will increase the sender's privacy by restricting the amount of information broadcast to the network.
>
> Even if you don't use complex wallet functionality like multisignature or Lightning, improving their privacy also improves yours, as it makes chain surveillance more difficult and increases the broader Bitcoin network anonymity set.

11. Whales can't get the face value of their HODL-ings. Last Friday the price crashed 20% in minutes. David Gerard writes:

> Someone sold 1,500 BTC, and that triggered a cascade of sales of burnt margin-traders' collateral of another 4,000 BTC. The Tether peg broke too.

That is 0.03% of the stock of BTC. Gerard writes:

> The real story is that the whales — "large institutional trading firms," ... want (or need) to realise the face value of their bitcoins, and they can't, because there just aren't enough actual dollars in the market. This is the same reason miners are keeping a "stockpile" of unsaleable bitcoins, as I've noted previously.
>
> So the whales are going to Goldman Sachs to ask for a loan backed by their unsaleable bitcoins, even though the collateral can't possibly cover for the value of the loan even if Bitcoin doesn't crash.

HODL-ers wishing to cash out face significant problems, as recounted by Harry Brennan in Harry Brennan's *'I made $4m profit on crypto, but the bank won't let me spend it'*:

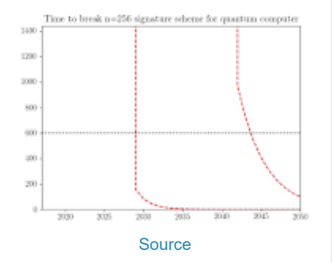
> Digital currency traders sitting on huge gains have been turned away by banks, with financial institutions fearing they may be unwittingly taking money from law breakers who use digital currencies to hide wealth illegally.
> ...
> Clive Gawthorpe of accountant UHY Hacker Young said traders face long waits of up to 24 months to access their own money, with tax an increasing concern for banks. "Every time they trade in and out of a coin they trigger a taxable event, some dating back years – and we are talking about thousands of transactions without proper record keeping," he said

12. Here is a list of institutions that a real-world user of cryptocurrencies as they actually exist cannot avoid trusting:
    - The owners and operators of the dominant mining pools not to collude.
    - The operators of the exchanges not to manipulate the markets or to commit fraud.
    - The core developers of the blockchain software not to write bugs.
    - The developers of your wallet software not to write bugs.
    - The developers of the exchanges not to write bugs.

    And, if your cryptocurrency has Ethereum-like "smart contracts":

    - The developers of your "smart contracts" not to write bugs.
    - The owners of the smart contracts to keep their secret key secret.

    Every one of these has examples where trust was misplaced.
13. In the medium term, Bitcoin and many other cryptocurrencies face two technological threats that might disrupt them and thus provide partial mitigation:
    - **Quantum computing**. *Quantum attacks on Bitcoin, and how to protect against them* by Divesh Aggarwal *et al* describes two threats they pose in principle:
        - They can out-perform existing ASICs at Proof-of-Work, but it is likely to be many years before this threat is real.
        - They can use Shor's algorithm to break the encryption used for cryptocurrency wallets, allowing massive theft. Aggarwal *et al* track the likely date for this, currently projecting between 2029 and 2044. When it happens there will be an estimated 4.6 million Bitcoins up for grabs.



Source

    - **The halvening**. At regular intervals Bitcoin's mining rewards are halved, with the goal that the currency eventually become fee-only.

Alas, Raphael Auer shows that a fee-only system is insecure.

Posted by David. at 5:00 PM
Labels: bitcoin

4 comments:

Conor said...

I know the talk was on mitigating externalities, but you do touch on a number of other areas and one thing you could add is a slide on the origin of money and why crypto is not a currency. The late David Graeber wrote a great book on debt, which posits money represents debt ownership.

February 11, 2022 at 3:38 AM

jerdavis said...

Sir, right off the top you lead with some dubious info.

The ewaste paper is generally discredited because of incorrect lifetime estimates.
25% of mining is still done by a 5 yo model (S9).
https://compassmining.io/education/bitcoin-hashrate-percentage-s9-asic/

For the energy FUD I refer you to the fine work of Nic Carter.
https://niccarter.info

Also the miningpool / 50% FUD is a fundamental misunderstanding of how mining pools work.
As a miner, it would only take me seconds to remove my hashrate from a bad pool, and advancements like stratum V2 make these attacks impractical.
https://braiins.com/stratum-v2

February 11, 2022 at 11:52 AM

David. said...

jerdavis, I see you rely on sources who are "talking their book". I prefer not to.

February 11, 2022 at 1:05 PM

David. said...

Some reactions to this talk on Twitter here, I love that it rated an "Old man yells at Bitcoin".

February 11, 2022 at 4:14 PM

Post a Comment

Home Older Post

Subscribe to: Post Comments (Atom)