ELECTRONIC FRONTIER FOUNDATION

House Committee on Energy and Commerce
Subcommittee on Innovation, Data, and Commerce

Hearing:
"Building Blockchains: Exploring Web3 and Other Applications for Distributed Ledger Technologies"

Statement of Ross Schulman
Senior Fellow, Decentralization
Electronic Frontier Foundation

June 7, 2023

EXECUTIVE SUMMARY

Blockchain is, at the end of the day, simply a clever means of structuring data that allows multiple parties to agree on the value of some object without trusting one another or having to trust a third party. It was designed to solve that particular problem, and it does so well. It is also useful in a handful of similar situations, but it is not as broadly applicable beyond that as the industry around it often claims.

It also has some particular drawbacks that are important to consider. For example, it is not inherently private. In fact, due to its transparent nature, private data should not be included in a blockchain, and there are ongoing projects that attempt to remedy this issue. Blockchains also deal with issues of inefficiency, both in the cost of operating them and in the throughput of the networks themselves.

In thinking about regulating blockchains, they should be treated much like any other tool would be. Normal consumer protections should apply to them, and Congress should pass a consumer driven comprehensive data privacy law, but blobkchain-specific legislation is unlikely to be necessary.

As Senior Fellow for Decentralization at the Electronic Frontier Foundation, I thank Chairmen Rodgers and Bilirakis, Ranking Members Pallone and Schakowsky, and Members of the Subcommittee for the opportunity to share EFF's views on blockchain. For over 30 years, as a member-funded non profit, EFF has represented the interests of technology users in both court cases and in broader policy debates to help ensure that law and technology support, and do not inhibit, our civil liberties. It is with that lens that we approach the question of blockchains and their uses.

What is Blockchain?

One of the first classes that an aspiring computer scientist takes at the beginning of their undergraduate studies is usually called something like "Data Structures and Algorithms." These are the fundamental building blocks of every computer program. Blockchains are, at their core, simply a new data structure. Like most technologies, they are not inherently good or evil. They are simply tools that provide particular features and have particular drawbacks. They do not require much in the form of targeted regulation beyond the standard consumer protections (though our country still desperately needs a consumer-driven baseline general privacy law), nor do they need particular nudging or assistance to be innovative.

Many barrels of ink have been spilled in the quest to explain how exactly blockchains work, so a full description here would be repetitive.[1] It is nevertheless worth delving into what, exactly, they are meant to accomplish.

The biggest problem that blockchains solve is providing a means for two or more parties to agree on the value of a piece of data when they do not trust one another and for whatever reason cannot

[1] Arvind Narayanan & Jeremy Clark, *Bitcoin's Academic Pedigree*, 60 Communications of the ACM 36 (2017).

or will not trust a third party to keep track of it for them.[2] In a non-blockchain system, those parties might rely on a bank or banking system, the system of legal contracts and the courts, a shared database perhaps combined with audits, or even just a handshake and a belief in one's fellow humans. Generally speaking, blockchains instead distribute the necessary trust across a network of peers in such a way that as long as 51% of the network acts honestly, the result can be relied upon.[3] In the context of a currency, this is often referred to as the "double spending problem," as the issue is making sure that someone has not spent something easily copyable like a digital currency in two different places. This feature is useful in more circumstances than blockchain's detractors claim it is, but in many fewer situations than the past few years' hype might lead one to believe.

There can be little question that the previous half-decade saw a hype and bust cycle surrounding blockchains, and cryptocurrencies in particular, that wildly inflated their actual monetary value as well as the public perception of their utility. While it may be premature to say that that cycle has now finished, it seems that the dust may be beginning to settle. In the clear-headedness that hopefully will follow, we will have an opportunity to assess where blockchain's strengths are well suited to actual problems that people face, and recognize those circumstances where they are not.[4]

---

[2] Andreas Antonopoulos, *Bitcoin security model: trust by computation*, O'Reilly Radar, (Feb. 20, 2014), http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html.
[3] Trail of Bits, *Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers*, (June 2022), https://blog.trailofbits.com/wp-content/uploads/2022/06/Unintended_Centralities_in_Distributed_Ledgers.pdf.
[4] Gregory Barber, *What's Blockchain Good for Anyway? For Now, Not Much*, Wired, (Oct 28, 2019), https://www.wired.com/story/whats-blockchain-good-for-not-much/.

What are Blockchains' Strengths?

In addition to the situations mentioned above, where two parties neither trust one another nor any available third party, blockchains have a few other strengths that might suggest them as a solution to particular problems. For one, blockchains make it easier to provide transparency and auditability of their contents.[5] This feature seems to lend itself to the record keeping of government documents, for example. And, indeed, there has been some work to apply blockchains to property deeds, though with varying success.[6] One could imagine a similar application for businesses' documents for audit purposes.[7] This same feature could potentially be applied to some legal proceedings where chain of custody is of the essence.[8]

Another area where blockchains may provide value are where they are tied into a system where they provide compensation for a service provided by the network itself. For example, the Filecoin blockchain uses a unique validation system called "Proof of Storage" in which nodes in the network are compensated for providing hard drive space to the network to be used as a storage back end similar to Amazon's S3 service.[9]

---

[5] Reid Blackman, *Why Blockchain's Ethical Stakes Are So High*, Harvard Business Review, (May 10, 2022), https://hbr.org/2022/05/why-blockchains-ethical-stakes-are-so-high.
[6] Gregory Barber, *What's Blockchain Good for Anyway? For Now, Not Much*, Wired, (Oct 28, 2019), https://www.wired.com/story/whats-blockchain-good-for-not-much/.
[7] Deloitte, The impact of blockchain technology on audit, https://www2.deloitte.com/us/en/pages/audit/articles/impact-of-blockchain-in-accounting.html.
[8] Jaliz Maldonado, *Chain of Custody for Evidence Using Blockchain Technology*, The National Law Review, (Sept 10, 2018), https://www.natlawreview.com/article/chain-custody-evidence-using-blockchain-technology.
[9] Filecoin, https://filecoin.io/.

There have also been efforts to incorporate blockchain into telecommunications infrastructure, such as the Althea project.[10] Althea is trying to build a mesh network in which neighbors can use a built-in blockchain to compensate each other for relaying their data over wireless networks.[11] Tying the payments layer to the service provided can make sense in circumstances like these, particularly where it enables microtransactions that would be untenable in another payment system and where it can be paired so closely with the service being provisioned.[12]

What are Blockchains' Limitations?

Blockchains also have a few important limitations that we should keep in mind:

First of all, blockchains are not inherently good for people's privacy. In fact, in their most basic form, such as implemented in the Bitcoin or Ethereum blockchains, they are affirmatively bad for privacy.[13] Every transaction conducted on those legers must be publicly posted, so that the whole network can analyze them for correctness and make sure that coins are not being duplicated.[14] While it is true that identities on these networks are pseudonymous–they are represented by long strings of letters and numbers–researchers as well as law enforcement entities, including the Federal Bureau of Investigation, have shown that transaction analysis can

---

[10] Althea L1 Blockchain, https://www.althea.net/blockchain.
[11] Transforming Connectivity | Althea, https://www.hawknetworks.net/
[12] *But see* Kyle Torpey, *Bitcoin is Now Useless for Micropayments, But Solutions Are Coming, Bitcoin Magazine*, (Mar 14, 2017), https://bitcoinmagazine.com/technical/bitcoin-now-useless-micropayments-solutions-are-coming1.
[13] Primavera De Filippi, *The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies*, Journal of Peer Production, (Sep 2016), http://peerproduction.net/editsuite/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/.
[14] *Ibid.*

easily pierce that privacy.[15] Indeed, to the extent that there is privacy on the blockchain, it is because it has been "bolted on" after the fact by projects such as Tornado Cash and ZCash.[16] We must be very careful in assessing the use of blockchains in situations where personal data may be involved, such as in social networking, data storage, or even in a system for tracking land ownership.

It is worth noting, as an aside, that those looking to solve this inherent problem with blockchains have helped to push forward the state of the art in cryptography in ways that have had benefits for privacy in other settings.[17] As an example, the privacy-focused ZCash project has pushed the development of Zero-Knowledge Proofs (ZKP) and their derivatives in ways that are useful to protect privacy in other circumstances.[18] For example, the Divvi Up project has created a way to collect analytics from software such as web browsers and mobile apps without exposing users' personal information, and is based on ZKPs.

Blockchain's second limitation is its relative inefficiency.[19] As many may already know, some blockchains require every node in the network to expend large amounts of resources in an effort

---

[15] Andy Greenberg, *Inside the Bitcoin Bust that Took Down the Web's Biggest Child Abuse Site*, Wired, (Apr 7, 2022), https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/.
[16] The Basics | Zcash, https://z.cash/the-basics/.
[17] Adrian Zmudiski, *The Future of Crypto: The Latest Cryptography Advances Set to Change Blockchain*, Cointelegraph, (Feb 20, 2020), https://cointelegraph.com/news/the-future-of-crypto-the-latest-cryptography-advances-set-to-change-blockchain.
[18] Karim Baghery, *ZK-SNARKs and Applications*, The ISC Webinar, (Nov 11, 2020), https://www.esat.kuleuven.be/cosic/wp-content/uploads/2020/12/ZK-SNARKs-and-Applications.pdf.
[19] Adam Levy, *5 Problems With Blockchain Technology*, The Motley Fool, (Jul 1, 2022), https://www.fool.com/investing/stock-market/market-sectors/financials/blockchain-stocks/problems-with-blockchain/.

to solve meaningless mathematical equations just to validate the next group of entries to be included in the ledger. This "Proof of Work" system is used in the Bitcoin network as well as a number of other networks, and leads to waste of energy and absurdly high transaction costs. At points the average cost to send a single transaction on the Bitcoin network reached as high as $60.[20]

In addition, the purposeful inefficiency tends to lead toward recentralization. As the research group Trail of Bits reported in a paper commissioned by the Defense Advanced Research Projects Agency (DARPA) from 2022, many of the largest blockchains are susceptible to attacks based on the fact that only a handful of entities comprise the majority of the deciding power in many of the largest blockchains. At the time of their writing, only four entities needed to collude to disrupt the Bitcoin blockchain. For Ethereum that number was only two.[21]

There have been efforts to solve these problems, most notably the move to "Proof of Stake" by the Ethereum blockchain in September of 2022.[22] Proof of Stake requires validators in the network to place into escrow, or "stake," a certain amount of value (usually in the form of the "coin" that the network uses). That stake is forfeited if the network determines that the validator

---

[20] Taylor DeJesus, *Bitcoin Transaction Fees: A Full Guide and How to Save*, Nasdaq, (Aug 26, 2022), https://www.nasdaq.com/articles/bitcoin-transaction-fees%3A-a-full-guide-and-how-to-save.

[21] Trail of Bits, *Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers*, (June 2022), https://blog.trailofbits.com/wp-content/uploads/2022/06/Unintended_Centralities_in_Distributed_Ledgers.pdf.

[22] Romain Dillet, *Ethereum switches to proof-of-stake consensus after completing The Merge, TechCrunch, (Sep 15, 2022),* https://techcrunch.com/2022/09/15/ethereum-switches-to-proof-of-stake-consensus-after-completing-the-merge/.

acted dishonestly.[23] This change eliminates the large inefficiencies in wasted electricity and, it is claimed, lowers the barrier of entry for validators by eliminating the large capital costs for hardware necessary in Proof of Work.

What Regulation Is Necessary?

In light of all of this, what should be the role of Congress in regulating blockchains? Broadly speaking, Congress should rely on the regulations that already exist to protect people. Much, if not most, of the harms that may arise from the use of blockchain are going to be well covered by the existing protections under authorities such as the Federal Trade Commission's Unfair and Deceptive Practices prohibition, other similar regulations at agencies like the Consumer Financial Protection Bureau, and state-level protections enforced by the various state Attorneys General or other state officials.[24] The two greatest things that Congress could do to protect Americans from harms related to blockchains would be to pass consumer driven comprehensive privacy legislation and to adequately fund the FTC so that it can hire the technical and legal experts it needs to properly investigate and prosecute those harms. It should also continue the ongoing work of making itself more familiar with technology through programs such as TechCongress and via resources within the Government Accountability Office, the Congressional Research Service, and others.

Since this Subcommittee is focused on innovation, it is also worth noting that regulation which targets the person who wrote a given piece of code, as opposed to those who take concrete action

---

[23] *Ibid.*

[24] *E.g.* Financial Technology, Federal Trade Commission, https://www.ftc.gov/news-events/topics/consumer-finance/financial-technology.

to cause harm, is bound to stifle innovation. Most blockchain projects are open source, and are the result of many individuals contributing small pieces to the overall whole.[25] If those contributors had to live in fear of the code they wrote landing them on the hook for later liability, development, and therefore innovation, would grind to an immediate halt.

Furthermore, one of the great strengths of open source software is that code under an open source license can be reused in other programs, sometimes without even the knowledge of the original author. That reuse is good for the software ecosystem at large, as it is more efficient to use an existing battle-tested piece of code to accomplish some task rather than rewriting it from scratch. If regulation aimed at blockchain were to assign liability to the authors of these other pieces of code merely included in a blockchain project, it could have negative repercussions not just within the blockchain space, but across all of open source development.

Conclusion

There can be no doubt that blockchain is a clever solution to the problem it was originally developed for: preventing someone from spending a unit of digital currency more than once without relying on a single point of trust. The overwhelming hype that this advancement has generated over the past years, however, has blinded many to the fact that its usefulness extends to one or two other use cases, but not all that much further. And that's ok. Hammers won't help you tighten a bolt but they're great when you need to drive a nail into some wood.

[25] Peter Van Valkenburgh, *What is "open source" and why is it important?*, Coin Center, (Oct 17, 2017), https://www.coincenter.org/education/advanced-topics/open-source/.

And, just as with other tools, regulating blockchain because it's blockchain would largely be counter productive. It is nearly always more appropriate to regulate the harmful actions than the tools used.

Thank you again for the opportunity to provide this testimony and I look forward to continuing to work with the Committee on these important questions.