Office of Science and Technology Policy
1600 Pennsylvania Ave NW
Washington, DC 20500
Re: Request for Information; Digital Assets Research and Development, January 26, 2023

March 3, 2023

Dear Colleagues,

Thank you for the opportunity to submit comments regarding the administration's interest in establishing a National Digital Assets Research and Development Agenda. The agency's request for information (dated January 26, 2023) seeks data and analysis regarding information on the potential benefits, risks and impacts of using digital assets and blockchain-based technology in fields beyond the financial sector, as well as ways in which further research and development could amplify such supposed benefits or mitigate risks and harms.

Americans for Financial Reform Education Fund (AFREF) is a nonpartisan, nonprofit coalition of more than two hundred civil rights, community-based, consumer, labor, small business, investor, faith-based, civic groups, and individual experts. We fight for a fair and just financial system that contributes to shared prosperity for all families and communities.

Demand Progress Education Fund (DPEF) works to elevate regulators who care more about the wellbeing of everyday people than Wall Street's bottom line, and fights to ensure that Congress conducts oversight to hold the financial sector accountable. We oppose deregulation and consolidation that makes our financial system less sound, and push back against attempts by the finance and tech sectors to normalize exploitative products and systems.

Summary

Our organizations are highly skeptical of the overall use case for crypto assets in a financial services context, especially considering the high degree of risk and harm posed by these assets as they are currently used. At a fundamental level, these products appear to have little current use beyond speculative investment – which some argue is essentially a form of gambling.[1]

While other submissions will no doubt focus on the purported or potential benefits of blockchain technology, this submission largely focuses on some of the limitations blockchain technology itself. Moreover, in this submission we urge the government to interrogate further the fundamental premise of this inquiry – that blockchain based technology is worth developing at scale, given the limitations of the technology and its value relative to alternative approaches.

[1] https://www.cnbc.com/2023/02/16/billionaire-charlie-munger-cryptocurrency-is-crazy-stupid-gambling.html

We offer here three categories of fundamental limitations or flaws found with blockchain technology – a non-exhaustive list – and provide an overview of analysis and criticism regarding these limitations which we believe raises serious questions. Following from that we offer a few broad recommendations regarding research and development informed by this critique.

Lastly, with respect to use of blockchain technology to create a US central bank digital currency (CBDC), our submission ends by summarizing concerns and recommendations regarding such a proposal that we provided to the Federal Reserve last year in response to a request for information regarding the Federal Reserve White Paper, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation" (January 2022). In short, we raise concerns about the impacts a CBDC might have on consumer and privacy rights and protections, and urge the Fed to consider non-blockchain based alternative technology for a digital dollar and other digital payment and banking systems.[2]

Introduction

Much has been written by academics,[3] public interest organizations,[4] industry observers[5], current[6] and former regulators[7], and others about the systemic problems found in the crypto asset industry, particularly in the wake of the recent collapse of Terra, FTX, and several other platforms, whose failure has driven losses of more than $2 trillion in crypto market value[8] and continues to negatively affect surviving platforms and crypto investors.

Some proponents of investing in blockchain technology acknowledge these flaws, but argue (among other points) that:

1. Blockchain is a new technology, and further development of it will resolve at least some of the flaws or limitations that currently cause or contribute to the problems found in the crypto industry and elsewhere.

2. Blockchain's key innovation is decentralization, and the benefit that decentralization brings alone is worth the resources needed to further develop the technology so it is viable and scalable for the long term.

3. The real, or perhaps more versatile application of blockchain, can be derived from its use not as a system of finance, but as a system used for information management – in short, as a database.

We believe each of the arguments are, at the very least, contestable, and may be fundamentally difficult to defend, based both on observable practices within existing blockchain infrastructure, and upon structural analyses of blockchain from various fields, including computer science, economics, and mathematics.

---

[2] https://ourfinancialsecurity.org/wp-content/uploads/2022/05/5.20.22-digital-assets-CBDC-letter.pdf

[3] https://www.banking.senate.gov/download/allen-testimony-12-14-22

[4] https://ourfinancialsecurity.org/2021/10/letters-to-regulators-letter-to-treasury-opposing-a-bank-charter-for-stablecoin-issuers/

[5] https://www.nytimes.com/2022/03/31/style/ben-mckenzie-crypto.html

[6] https://www.reuters.com/technology/us-sec-chair-gensler-calls-congress-help-rein-crypto-wild-west-2021-08-03/

[7] https://www.linkedin.com/pulse/fraudulent-design-language-cryptocurrency-john-reed-stark/?published=t

[8] https://www.cnbc.com/2022/12/23/bitcoin-lost-over-60-percent-of-its-value-in-2022.html. Note: estimates of crypto market values, market capitalization, etc., vary and are not well defined.

Below we share some of the literature and analysis available that calls into question these arguments, which often form the basis of the rationale for the continued prioritization of investment in blockchain technology.

1. Blockchain Technology Is Not New

Blockchain proponents often argue that the technology is still in the "early days" of its development. This claim is used either offensively – to suggest that the technology offers significant unrealized potential benefits that will emerge in the near future – or defensively, to explain why the consistent failures of blockchain-based technology are not indicative of its enduring limitations but constitute "growing pains" that are a natural and necessary phase in the technology's development.

A relatively well-known essay by Molly White, a software programmer and noted critic of crypto assets and blockchain, entitled, "It's not still the early days" lays out the basics of a rebuttal to this argument.[9] In summary, White points out that Bitcoin was launched in 2009; Ethereum in 2015. Many first generation and second generation blockchain applications are anywhere from 7-13 years old. During that same time range, numerous other technological products and platforms (some new, some established) have been further developed and achieved stable, widespread use more rapidly. These products include things as varied as major social media platforms, online ride-sharing apps and platforms, new computer processors, new database programs, programming languages, operating systems, payment apps, and more.

While the nature of these innovations vary widely (and bring with them their own variety of benefits and negative externalities, some of which are profound in scope and are a core focus of our advocacy efforts), what they have in common is that arguably, they have all demonstrated their relative utility, scalability and viability in a relatively short period of time. In contrast, crypto and blockchain products have not demonstrated nearly the same levels of uptake within a similar time frame.

For example, in the payments sector, blockchain-based crypto assets struggle to demonstrate their usefulness as a mainstream method of payment (though anecdotal references to their usefulness in remittances or aid-based money transfers are ubiquitous.) Yet non-blockchain based digital payment systems have appeared to flourish more quickly and more broadly. Brazil's digital payment system Pix, introduced in 2020, now has more than 127 million Brazilians and more than 10 million companies as subscribers or users.[10] Africa's M-Pesa mobile phone payments service, introduced in 2007, has expanded to 10 countries, has 29.5 million active users and processes up to 614 million transactions per month.[11] These systems have their own unique weaknesses and risks they pose from a public interest standpoint (some of them significant), but from a technological and service delivery standpoint their use cases are much clearer and stronger than what blockchain-based technologies have been able to demonstrate.

White writes, "One only needs to look at Moore's law to see how this is pretty much built into the technology world, as once-impossible ideas are rapidly made possible by exponentially more processing power. And yet, we are to believe that as technology soared forward over the past decade, blockchain technologies spent that time tripping over their own feet?"

[9] https://blog.mollywhite.net/its-not-still-the-early-days/

[10] https://www.bloomberg.com/news/articles/2022-11-23/brazilians-choose-central-bank-s-payment-app-over-credit-cards?sref=f7rH2jWS

[11] https://africa.businessinsider.com/local/markets/m-pesa-kenyas-mobile-money-success-story-celebrates-15-years/srp9gne

Some trace the lineage of the building blocks of cryptocurrency and blockchain (distributed ledgers and encryption) even further back to the 1980s or 1990s, depending on where one starts in the chronology, with products such as eCash, eGold, BitGold.[12] Following this line of association, this area of technology has had an even longer head start, and yet has not scaled or progressed at comparable pace or level to other technological advancements.

Naturally, not all innovation or invention proceeds along a neat line of progression. It is theoretically possible that someone will develop a 'killer app' based on blockchain technology at some point.[13] However, the question remains, why prioritize development of a technology that has clear structural flaws which have impeded its development for arguably 30 years or more, especially when superior alternatives exist?

As Kai Stinchcombe, a tech writer and founder of financial services firm argues (referring to blockchain technology's utility in terms of data storage and distribution),

> "There are four additional problems with a blockchain-driven approach. First, you're relying on single-point encryption — your own private keys — *rather than a more sophisticated system* that might involve two-factor authorization, intrusion detection, volume limits, firewalls, remote IP tracking, and the ability to disconnect the system in an emergency. Second, price tradeoffs are entirely implausible — *the bitcoin blockchain has consumed almost a billion dollars' worth of electricity to hash an amount of data equivalent to about a sixth of what I get for my ten dollar a month Dropbox subscription*. Fourth [*sic*][14], systematically choosing where and how much to replicate data is an advantage in the long run — *the blockchain's defaults on data replication just aren't that smart.* And finally, Dropbox and Box.com and Google and Microsoft and Apple and Amazon and everyone else provide a set of valuable other features that you don't actually want to go develop on your own. Analogous to Visa, the problem isn't storing data, it's managing permissions, un-sharing what you shared before, getting an easy-to-view document history, syncing it on multiple devices, and so on.
>
> The same argument holds for proposed distributed computing and secure messaging applications. *Encrypting it, storing it forever, and replicating it across the entire network is just a ton of overhead relative to what you're actually trying to accomplish. There are excellent computing, messaging, and storage solutions out there that have all the encryption and replication anyone needs — actually better than blockchain based solutions* — and have plenty of other great features in addition (emphasis added)."[15]

---

[12] https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/#:~:text=The%20first%20cryptocurrency%20was%20eCash%2C%20created%20by%20David%20Chaum's%20company,very%20influential%20in%20Bitcoin's%20creation.

[13] Some argue that blockchain, or more specifically Bitcoin, is that 'killer app,' in terms of how it combines these technological precursors in modestly novel ways that have solved problems earlier models faced. The challenge with this argument is that even if one assumes Bitcoin may do one thing well - establish a 'censorship resistant' method of exchanging digital assets - the methods it uses to accomplish this - decentralized consensus mechanisms, etc. - generate massive negative externalities and may stunt the development of other ways in which blockchains might be used.

[14] The author actually makes three points in this excerpt but misnumbered the points in the original text.

[15] https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100; additionally the data used to calculate the electricity use in this example is circa 2017. It is generally understood that the electricity demands of PoW systems remain large and inefficient.

If the core elements of blockchain technology are not wholly "new" and by inference truly disruptive in nature, and the progression of the technology is slow relative to other tools with similar attributes developed in parallel that provide similar services with more real benefits and fewer challenges, and the technology itself has structural limitations (along with significant externalities and associated risks), it begs the question, is this an innovation worth prioritizing, given these limitations and the very real risks and harms that are present today as the technology is used? As software engineer Luke Plant (whose work is described further below) writes, "There are plenty of new technologies that turn out to be duds."[16]

2. Blockchain Platforms Are Not Truly Decentralized

Defenders of blockchain technology will sometimes acknowledge the real limitations of its design but suggest that blockchain's key innovation – decentralization – is worth "selecting" for. David Rosenthal, a well-known computer scientist and critic of blockchain technology,[17] has written extensively on this matter.[18] In one publication, Rosenthal points to the writings of Albert Wenger (drawing on Clayton Christensen), who, while attempting to defend blockchain technology, made a comparison between blockchain and PCs:

> "The canonical example here is the personal computer (PC). The first PCs were worse computers than every existing machine. They had less memory, less storage, slower CPUs, less software, couldn't multitask, etc. But they were better at one dimension: they were cheap. And for those who didn't have a computer at all, that mattered a great deal."
>
> ...
>
> A blockchain is a worse database. It is slower, requires way more storage, and compute, doesn't have customer support, etc. And yet it has one dimension along which it is radically different. No single entity or small group of entities controls it."[19]

Wenger goes on to say that a decentralized platform like blockchain could be the basis for an internet not controlled by centralized corporations (e.g., web3) and that if the technology is widely adopted economies of scale will emerge that will either solve or incentivize solutions to make such tech faster, safer, more efficient – all because the innovative value of decentralization provides enough utility to make all this worth it.

Rosenthal offers two critiques of this position. First, he notes that "the infrastructure of the internet (IP/DNS/HTTP and so on) is decentralized, but that hasn't stopped the actual internet everyone uses being centralized." Two, in large part, blockchains as they operate now are not actually decentralized. Three key data points Rosenthal raises help bear this out:

- Concentration of control of crypto mining operations amongst a few key mining pools;
- Concentration of crypto trading activity on one key platform (Binance); and
- Concentration of Bitcoin holders, with a very small portion of wallets holding a large percentage of Bitcoin in circulation.

[16] https://lukeplant.me.uk/blog/posts/the-technological-case-against-bitcoin-and-blockchain/#the-problem-with-technology
[17] https://en.wikipedia.org/wiki/David_S._H._Rosenthal
[18] https://blog.dshr.org/
[19] https://blog.dshr.org/2022/01/blockchain-gaslighting.html

The data supporting Rosenthal's points has not substantively changed since his writing in January 2022. As of January 2023, two mining pools controlled 51% of Bitcoin's hash rate (with similar levels of concentration found on other chains);[20] 66.7% of all crypto trading on centralized exchanges (which themselves constitute the bulk of all crypto trading) now occurs on Binance;[21] and as of July 2022 one analysis determined that .04% of BTC addresses (or wallets) held 62.25% of all Bitcoins issued.[22] Other sources have offered confirmation of this ongoing trend of centralization - for example, a recent Wall Street Journal article revealed how a group of roughly half a dozen coders "serve as stewards of Bitcoin Core, an open-source program that keeps the cryptocurrency's digital ledger up-to-date on thousands of computers that make up its network."[23]

Another recent study further demonstrates how existing blockchains are not nearly as decentralized as presented, are at risk as a result, and may face structural challenges in achieving "true" decentralization. Trail of Bits is a New York-based firm that provides security assessments and advisory services to major information technology companies. The firm was engaged by the Defense Advanced Research Project (DARPA) to investigate the extent to which blockchains are truly decentralized. Their study, published in July 2022, focused on Bitcoin and Ethereum (two largest and most popular crypto blockchain platforms).[24]

Their report found that, though the cryptographic tools used to secure blockchain's immutability were robust (a feature which helps promote decentralization), the platforms they surveyed were vulnerable to exploits that took advantage of their chain's other properties – their implementation approaches, networks and consensus protocols. A few examples among many:

- Every widely used blockchain has a privileged set of entities that can modify the semantics of a blockchain to potentially change past transactions.
- The number of entities sufficient to disrupt a blockchain is relatively low: four for Bitcoin, two for Ethereum, and less than a dozen for most PoS (Proof of Stake) networks.
- A dense, possibly non-scale free, subnetwork of Bitcoin nodes appears to be largely responsible for reaching consensus and communicating with miners – the vast majority of nodes do not meaningfully contribute to the health of the network.
- Bitcoin traffic is unencrypted - any third party on the network route between nodes (e.g., ISPs, Wi-Fi access point operators, or governments) can observe and choose to drop any messages they wish. Additionally, of all Bitcoin traffic, the researchers found that for extended periods of time, 60% of such traffic traverses just three ISPs.

The study identifies many more vulnerabilities. Taken as whole, the picture it paints is that not only do these flaws demonstrate that existing blockchains are vulnerable to "centralized" attacks or exploits, but that a) some of these flaws will be difficult to fix with simple technology, due to the incentive structures found within blockchain based consensus mechanisms, and b) these networks are at present time operating in de facto centralized manner.

---

[20] https://cryptoslate.com/behind-the-two-mining-pools-controlling-51-percent-of-the-global-hash-rate/
[21] https://cryptonews.com/news/binance-has-grabbed-two-thirds-of-all-crypto-trading-volume-what-happened-to-the-decentralization-of-finance.htm
[22] https://cointelegraph.com/news/hodlers-and-whales-who-owns-the-most-bitcoin-in-2022
[23] https://www.wsj.com/articles/bitcoin-core-maintainers-crypto-7b93804
[24] https://assets-global.website-files.com/5fd11235b3950c2c1a3b6df4/62af6c641a672b3329b9a480_Unintended_Centralities_in_Distributed_Ledgers.pdf

To be clear, in pointing out the lack of decentralization found in blockchain-based platforms and the barriers to such decentralization, we are not taking the position that decentralization via blockchain is necessarily a worthy goal.[25] Rather, we are taking blockchain proponents' arguments at face value: that decentralization is the key value-add provided by blockchain technology that is worth "selecting for" in spite of current and future drawbacks and challenges. If decentralization isn't actually meaningfully present in these systems, and a combination of technological and economic factors making achieving real decentralization difficult or impossible, or not worth the cost relative to other alternatives, then it raises the question of whether blockchain technology is worth developing relative to other approaches.

3. Permissionless Blockchains are Difficult to Disentangle from Financialization

Applications of blockchain technology outside the financial services sector theoretically rely less on the notional utility of "digital assets" created and stored on blockchains, and more on the utility of the underlying distributed database itself. As such, some argue that the threat/benefit profile of blockchains may be different from those found in the financial services, and thus observers should distinguish between and differentiate "crypto" from "blockchain".

Arguably, however, it can be difficult to divorce the use of distributed ledger technology from the practice of tokenizing data on such a database, and its subsequent monetization or use as a financial instrument.

UK-based software engineer Luke Plant, who has written an extensive analysis identifying the design flaws and limitations of blockchain technology, points out that, at least for permissionless (public) blockchains, "Note also that you can't remove the cryptocoin and keep the blockchain technology – a permissionless blockchain requires a speculative cryptocoin to power it, otherwise no-one will ever pay for it." Plant elaborates further by quoting David Rosenthal, who argues:

> "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."

There may be current or future applications of blockchain technology which are able either disprove this argument or find workarounds that don't negate the value of using a blockchain/DLT based platform (either by introducing a third party or making the platform insecure). And, as explored briefly below, some blockchain proponents argue that the financialization of various types of data is what "powers" certain blockchain operations and produces "value" from them.

But Plant and Rosenthal's point raises a serious challenge - if permissionless systems rely on decentralized consensus mechanisms to perform their core function(s), and those consensus mechanisms must rely on financial or economic incentives to work, the deployment of blockchain, even

[25] Other proposals exist to achieve decentralization in the context of information technology platforms. For example, Tim Berners Lee (widely credited with being a founder of the world wide web) has offered an approach he deems Web 3.0 - https://www.cnbc.com/2022/11/04/web-inventor-tim-berners-lee-wants-us-to-ignore-web3.html. We take no position at this time on the merits of this approach or otherwise. But, we share it to make the point that if 'decentralization' is a worthy aim, technologists can and should explore with a critical eye different pathways to achieve it. Yet the discourse on blockchain often already assumes that blockchain is 'the' path to decentralization and that developmental pathways to achieve it must flow from there.

for purposes primarily other than financial products and services, may nearly always include some element that relies on speculative financial activity.

For our organizations, that suggests the risks present in such speculative financial activities will often increase the risk profile of blockchain technology deployments, and increase the complexity of identifying appropriate regulatory and oversight mechanisms – all of which expend money, time, and resources that could otherwise be spent on alternative technologies that could achieve similar objectives.

Central Bank Digital Currencies (CBDCs)[26]

Proposals for a CBDC assume that a digital dollar built using blockchain technology and its associated institutional architecture may be able to address key financial inclusion issues, such as lack of access to bank accounts, the need for faster, more secure, and reliable payment systems, etc., and can do so while offering sufficient privacy and consumer protections for CDBC holders and users.

However, A CBDC (in general, or a poorly designed/deployed one) might: 1) Expose users to expansive surveillance activities and undue violations of privacy; 2) Undermine access to and availability of physical cash; 3) Push the Fed to take more of a role in the economy and financial markets than may be wise, either by buying more assets to offset CBDC liabilities, or by exercising more control over bank's debt and credit decisions, constraining banks' and consumers' access to credit; 4) Impact funding or support for the community reinvestment act (CRA) program, negatively impacting access to banking services for low income communities; and 5) Be used or abused to unfairly restrict people's use of public benefits, or to garnish wages to serve private or government debts.

For these reasons we have urged the Fed, and encourage your office, to reconsider the fundamental premises behind a CBDC and work with other agencies to make room for a more polycentric institutional and technological architecture, which may or may not incorporate blockchain-based tokens, if they prove to be as or more effective than other option and do not present comparatively higher risks.

Indeed, such architecture could incorporate both existing Fed systems and new innovative approaches that are not dependent on DLT technology. For example, we would support the acceleration of the Fed Now program, with consumer fraud protections incorporated, which would expand the availability of real-time payments as a first step. We would additionally see promise in the deployment of a privacy-protecting Fed Accounts system that would expand the capacity of the Fed to provide account-based deposit and payment systems, with low or no fee services, beyond commercial banking institutions to retail customers. Such a system could be coupled with proposals to implement a postal banking program where the post office, which already provides payments-based services such as money orders, could serve as a front-end point of contact for retail users.

Finally, we support proposals to create "e-cash" – offline, hardware-based digital cash, built using existing technology, and issued by the Fed, Treasury or some combination of agencies – that could serve the same function as physical cash, without the risks to privacy, consumer fraud and structural imbalances that a Fed-issued, blockchain based digital currency may present. Indeed, such systems already exist outside the US, where payment systems using SIM-card based hardware tied to mobile phone platforms are a popular means of making payments. Card and chip-based hardware already in

[26] For more extensive commentary from our organizations on CBDCs and digital dollar proposals, including a brief discussion of potential design principles for a CBDC, please refer to our May 2022 submission to the Federal Reserve - https://ourfinancialsecurity.org/wp-content/uploads/2022/05/5.20.22-digital-assets-CBDC-letter.pdf

use for commercial smartcards and U.S. military payments technology could be modified or altered to serve as digital cash, and there are many measures that could be employed to ensure the safety, security and authenticity of such digital cash using existing or modified technology to make such e-cash comparable to paper cash by these measures.

Despite the concerns listed above, we do believe it is worth exploring how a CBDC might be developed, for two reasons. First, within the framing we describe above, a comparative analysis of different approaches and modalities for a digital dollar could help better demonstrate either how heterogenous tools could complement one another, or how deployment of non-blockchain approaches could obviate the need for a blockchain-based digital dollar. Such an analysis might also identify the extent to which the risks posed by a CBDC could, or could not be mitigated, either by technological, policy or legal solutions. The danger in not fully mapping these scenarios is that the most ardent proponents of a CBDC may be tempted to engage in wishful or magical thinking about potential adverse consequences rather than seek clearly identify and take meaningful steps to prevent or mitigate them. OSTP and other agencies should instead conduct rigorous due diligence on any proposals before they are approved and deployed.

Second, we are deeply skeptical of the notion that privately created and circulated cryptocurrencies are a viable alternative to a CBDC/public digital dollar. Digital assets have flaws and vulnerabilities too numerous to name in full, but the concerns we and many others have about these assets' security, reliability, volatility, stability, and viability as payment systems should be enough to move federal agencies to keep private digital assets largely "off the table" as a realistic solution for financial inclusion. As such, exploration of a public digital dollar, either as a CBDC or not, may help ensure that federal agencies do not cede too much ground to this idea, and instead remain focused on ensuring the federal government is upholding its responsibility to provide a public currency and payments system that is equitable, reliable, efficient, safe and secure.

Recommendations

Our overarching recommendation for this research and development agenda is that, to the extent practical or feasible within the OSTP's mandate, it should be organized around concrete objectives first (those given in the initial request for information from the OSTP are good illustrative examples of objectives that might serve), and that a comparative analysis is then done from a more technology neutral or agnostic standpoint, to evaluate both blockchain-based and non-blockchain based technological solutions on equal footing.

We believe this reorientation could be a more fair and objective approach, and provide some compensation for a dynamic commonly identified by observers of this industry, who point out that blockchain is often a "solution in search of a problem."[27]

Additionally, the OSTP should strive to ensure that stakeholders, participants and evaluators of research initiated under this agenda are drawn from a diverse pool of individuals and entities whose perspectives and expertise can meaningfully represent different and independent viewpoints on the proposed merits, flaws, or limitations of blockchain technology.

[27] Letter in Support of Responsible Fintech Policy - https://concerned.tech/

In June 2022, a group of more than 1500 technologists, many with distinguished backgrounds in the fields of computer science and software engineering, signed and sent a letter to Congress, calling on policymakers to "take a critical, skeptical approach towards [crypto industry] claims" and to "take an [policymaking] approach that protects the public interest and ensure technology is deployed in genuine service to the needs of ordinary citizens."

These technologists created and signed this letter due to concerns that policymakers were receiving a lopsided representation of technologists' views regarding blockchain technology, which was at odds with their views on the matter:

> "By its very design, blockchain technology is poorly suited for just about every purpose currently touted as a present or potential source of public benefit. From its inception, this technology has been a solution in search of a problem and has now latched onto concepts such as financial inclusion and data transparency to justify its existence, despite far better solutions to these issues already in use. Despite more than thirteen years of development, it has severe limitations and design flaws that preclude almost all applications that deal with public customer data and regulated financial transactions and are not an improvement on existing non-blockchain solutions."

Despite their conviction and depth of understanding, we suspect none of these signatories would argue their expertise here is utterly infallible, and we certainly hope proponents of blockchain technology believe the same about their own views and analysis. Scientific inquiry benefits from dissent and disagreement. We hope that the research initiatives spurred by the OSTP and its initiative here provide ample space for such discourse, and thank you once again for the opportunity to share our views on this subject.

Sincerely,

Mark Hays
Senior Policy Analyst
Americans for Financial Reform Education Fund
Demand Progress Education Fund

For any questions or comments about this submission,
Please contact submission author Mark Hays, Senior Policy Analyst with AFREF/DPEF,
markhays@ourfinancialsecurity.org