MERCATUS CENTER
George Mason University

PUBLIC INTEREST COMMENT

MARKET-BASED SOLUTIONS CAN BUILD PUBLIC TRUST IN DECENTRALIZED FINANCE

AGNES GAMBILL WEST
Visiting Senior Research Fellow, Mercatus Center at George Mason University

Ensuring Responsible Development of Digital Assets; Request for Comment
Agency: US Department of the Treasury
Comment Period Opens: July 8, 2022
Comment Period Closes: August 8, 2022
Comment Submitted: August 8, 2022
Document No. 2022-14588

I appreciate this opportunity to respond to the US Department of the Treasury's July 8, 2022, request for comment, "Ensuring Responsible Development of Digital Assets." The Mercatus Center at George Mason University is dedicated to bridging the gap between academic ideas and real-world problems and to advancing knowledge about the effects of regulation on society. This comment, therefore, does not represent the views of any party or special interest group. Rather, it is designed to inform the Treasury about certain risks and opportunities that the development and adoption of different types of digital assets might present to US consumers, investors, and businesses.

This comment focuses on market-based solutions, including accreditation and consumer education, to mitigate risks to the public that might arise through engagement with digital assets. This comment also discusses how adoption of digital assets creates opportunities for philanthropy.

RISKS

SECTION D(5)(A)

Frauds and scams in the decentralized finance (DeFi) ecosystem present financial risks to consumers and investors. In 2021, approximately $7.8 billion of cryptocurrency was stolen as a result of scamming activity.[1] Of this, over one-third came from a type of scam called a "rug pull." There are many types of rug pulls. One is when developers build a seemingly authentic DeFi project to attract investors before disappearing with their funds.[2] Another can be "pump and dump" schemes, where developers launch a

[1] Chainalysis, *The 2022 Crypto Crime Report*, February 2022, 5, https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf.
[2] Chainalysis, *The 2022 Crypto Crime Report*.

The ideas presented in this document do not represent official positions of the Mercatus Center or George Mason University.

new cryptocurrency, hold a significant percentage of that cryptocurrency until they pump up the price using marketing and promotion by social media influencers, and then dump it, causing a severe drop in its value—often to zero.[3] Another type is when a developer codes cryptocurrency tokens so that only certain parties, often insiders, can sell them.[4] The launch of the Squid Game (SQUID) token is a notable example of this phenomenon. SQUID experienced 45,000 percent growth in a few days but left investors unable to sell their tokens due to an anti-dump mechanism that was described in its white paper and present in the cryptocurrency's code.[5]

Rug pulls result in losses for investors through the erasure of an asset's value. Frauds and scams create reputational harm for the DeFi industry as a whole and damage the credibility of legitimate projects. They also create mistrust with the public, which may be unwilling to invest or participate in the digital asset ecosystem because of these looming risks and the dearth of tools available to assess these risks in the marketplace.

To achieve mass participation, the public must be able to trust and verify that its investments and consumer activities are protected from harm. Market-based solutions are uniquely able to achieve this goal. For example, participants in the DeFi ecosystem could establish one or more accreditation bodies that provide formal, third-party code audits of DeFi projects. For example, Underwriters Laboratories, Inc. is a nonprofit organization that advances standards development and investigates risks of new technologies, such as artificial intelligence and autonomous systems.[6] Its work has accelerated safe scientific discovery and informed public policy about the threats of technological change.[7]

Accreditation of DeFi projects from a similar type of organization could serve as a gold standard. It would serve as a signal to the public that a particular DeFi project does not have any security loopholes that would allow malicious actors to exploit investor and consumer funds.[8] Accredited third-party code audits are important because the public may not know how to analyze code for errors or scams. Accredited code audits could also be required before a token can be listed on an exchange or accepted as a form of payment.

SECTION D(5)(C)

Public and private keys are core components of cryptocurrencies. They allow individuals to send and receive cryptocurrency funds securely without third-party verification of the transaction.[9] Private keys are a string of alphanumeric characters that are mathematically generated from a related public key.[10] Barring quantum computing algorithms that may be able to unlock asymmetric key cryptography, private keys are

[3] Lisa Ferber, "How Crypto Investors Can Avoid the Scam That Captured $2.8 Billion in 2021," *NextAdvisor*, April 19, 2022.

[4] Elnaz Sarraf, "How to Avoid Crypto Rug Pulls in 2022," *HackerNoon*, April 25, 2022.

[5] Helen Partz, "Users Unable to Sell Squid Game Token Clocking 45,000% Gains," *CoinTelegraph*, October 29, 2021.

[6] UL Solutions (website), accessed August 4, 2022, https://www.ul.com/.

[7] Underwriters Laboratories, "Underwriters Laboratories Announces $1.8 Billion Commitment to Safety Science Research," news release, February 7, 2022, https://www.prnewswire.com/news-releases/underwriters-laboratories-announces-1-8-billion-commitment-to-safety-science-research-301476616.html.

[8] Elliptic, *DeFi: Risk, Regulation, and the Rise of DeCrime*, November 18, 2021. According to Elliptic, scams and rug pulls are challenging to identify and distinguish from code exploits, economic exploits, and admin key exploits. Code exploits are when developers intentionally introduce bugs into DeFi protocols to allow their creators to open a "back door" to steal user funds.

[9] "What Are Public and Private Keys?," *Cryptopedia*, Gemini, June 28, 2022.

[10] "What Is a Private Key?," Coinbase, accessed August 4, 2022, https://www.coinbase.com/learn/crypto-basics/what-is-a-private-key.

nearly impossible to reverse engineer.[11] This means that individuals who lose their private key lose access to their funds, which is a risk for consumers, investors, and businesses.

Some individuals may choose to assign a custodian to store their keys on their behalf. In this case, the custodian can help recover lost keys or regain access to a wallet.[12] With self-hosted wallets, however, there is no third party to perform this recovery function.[13] The public needs to be informed about the risks involved with using self-hosted wallets and about how to manage and store private keys. As the DeFi industry evolves, new backup mechanisms are likely to be developed beyond, for example, the multiword secret recovery phrases (or “seed phrases”) that are widely used today.[14] In order for this process of creative destruction to occur, private industry needs to continue to invest in research and development, and reduced regulatory burdens would allow for experimentation and transformative growth by innovative startups.

OPPORTUNITIES

SECTION B(3)(A), SECTION B(3)(C), AND SECTION B(3)(D)

Digital assets, and the technical framework that underpins them, hold the potential to create new opportunities for capital formation and fundraising for different sectors of the economy. One area that has benefited from the democratizing features of the digital asset marketplace is philanthropy.

Decentralized nonprofits and donor-advised funds (DAFs) are two types of entities that orchestrate geographically disparate groups to raise philanthropic funds quickly, often in the form of digital assets. Some of these entities are decentralized autonomous organizations (DAOs) that run on the Ethereum blockchain and are defining the next frontier of philanthropy.[15] Entirely digital in form, philanthropic DAOs can bring together a community of donors who in turn give digital assets to a DAF or a grant-focused community fund. Once the donor funds are pooled together, the community can collectively decide on where distributions or grants would make the greatest impact to society.

The pooling feature of DAO-enabled DAFs is important, given that it allows any donor to make any contribution in cryptocurrency, regardless of the size of the donation. Furthermore, the DAO community governance model is an alternative to the top-down approach of relying on trustees, board members, and nonprofit management to make funding decisions, a process that often lacks transparency.[16] DAOs may

[11] “The National Institute of Standards and Technology (NIST) predicts that quantum computers will be fully operational in a decade, and they will be able to break asymmetric key cryptography.” Joseph Stephen Savariraj and Sergio de Simone, “An Introduction to Post-Quantum Public Key Cryptography,” *InfoQ*, February 11, 2022.

[12] “Custodial Wallet,” Coinbase, accessed August 4, 2022, https://help.coinbase.com/en/coinbase/getting-started/crypto-education/glossary/custodial-wallet.

[13] “Custodial vs. Non-Custodial Wallets,” *Cryptopedia*, Gemini, May 6, 2021.

[14] A “seed phrase” is a series of 12–24 words that a wallet holder must remember to access an inaccessible account. It is also called a “recovery seed.” “How to Back up Your Hardware Wallet: Best Practices,” *Cryptopedia*, Gemini, March 10, 2022; SatoshiLabs, “Broken Hardware Wallet? Don’t Panic!,” *Trezor Blog*, September 1, 2021. One possible solution to the problem of lost keys is “social recovery wallets.” Vitalik Buterin, “Why We Need Wide Adoption of Social Recovery Wallets,” Vitalik Buterin’s Website, January 11, 2022, https://vitalik.ca/general/2021/01/11/recovery.html.

[15] Endaoment (website), accessed August 4, 2022, https://endaoment.org/; “Ten DAOs Disrupting the Social Impact Space,” *Crypto Altruism*, November 19, 2021; and Big Green DAO (website), accessed August 4, 2022, https://dao.biggreen.org/.

[16] Paul Brest notes differences between top-down and grassroots philanthropy in “Top-Down and Bottom-Up,” *HuffPost*, December 21, 2008.

also leverage features of the digital asset ecosystem, such as multisignature treasuries and multigovernance voting systems, to engage in collective decision-making.[17]

In addition, the relative ease of use and transfer speed of digital asset payment methods have the potential to further transform and democratize philanthropy by reaching a geographically and socioeconomically diverse group of donors and grantees. Crypto donations are already rising annually.[18] For example, in 2021, nonprofits received a total of $69.64 million in crypto donations via The Giving Block, which represents an increase of 1,558 percent from 2020.[19] Social impact investing can also benefit from the rapid, unencumbered process of capital formation that the DeFi ecosystem provides.

CONCLUSION

Although the growth in digital asset adoption may increase the risk of financial crime, including frauds and scams, market-based solutions can be developed to mitigate these risks. Accrediting bodies could be used to vet DeFi projects, and consumer education can inform cryptocurrency users of the benefits and risks of storing their funds in a custodial wallet as opposed to a self-hosted wallet.

Philanthropic use adds an important dimension to the digital asset ecosystem. When crafting regulations for the relatively nascent digital asset sector, regulators should not only consider the potential risks but also the opportunities that decentralized systems can create for positive societal change.

[17] BigGreen DAO (website).

[18] The Giving Block, *2021 Annual Report*, 2021.

[19] The Giving Block, *2021 Annual Report*.