Peter Van Valkenburgh[1]

Director of Research at Coin Center

RESPONSES TO QUESTIONS FOR THE RECORD

"America on "FIRE": Will the Crypto Frenzy Lead to Financial Independence and Early Retirement or Financial Ruin?"

June 30, 2021

Questions for Mr. Peter Van Valkenburgh, Director of Research, Coin Center, from Representative Warren Davidson:

- **Does the composition of the underlying assets of USDT make it a security? What are the investor protections in place for counterparty risk of insolvency in stablecoins?**

The definition of a security in US law is inherently flexible and fact intensive. Stablecoins, USDT among them, are not a homogenous product type. The facts of any particular stablecoin issuance will determine whether it is or is not a security under US law, and it is very possible—if not likely—that some stablecoins will qualify as securities while others will not. The definition of a security in the relevant statutes includes the terms "investment contract" and "note" and these terms have, in the past, been further clarified through the courts. The most relevant cases are *SEC v. Howey*,[2] from which the "*Howey* test" for an investment contract is derived, and *Reves v. Ernst & Young*,[3] from which the "*Reves* family resemblance test" for notes is derived. Neither of these cases, however, dealt with digital assets or stablecoins specifically so we can only reason by analogy. Because this an area of genuine uncertainty regarding underlying law and interpretation, ultimately, only a judge will be able to decide. Key factors from prior case law that will be relevant to that judgement include:

---

[1] Peter is Director of Research at Coin Center, the leading independent non-profit research and advocacy group focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. http://coincenter.org

[2] *SEC v. Howey*, 328 U.S. 293 (1946).

[3] *Reves v. Ernst & Young*, 507 U.S. 170 (1993).

A. Whether there is a regulatory regime already in place that mitigates the risks to persons holding the stablecoin (an important factor in the *Reves* family resemblance test).[4] We note that some stablecoins are issued by chartered trust companies and licensed money transmitters that are supervised by US state banking regulators. This supervision may mean that such stablecoins are not securities. Other stablecoins are issued by off-shore entities that may not have comparable supervision and these may be found to be securities.

B. Whether the issuer of the stablecoin exercises ongoing entrepreneurial or managerial discretion in selecting which assets should back the value of the stablecoin at any particular time (a factor in the *Howey* test).[5] We note that some stablecoins are backed by a limited category of low risk assets approved by a regulatory authority while others are backed by commercial paper or other riskier assets chosen by the issuer outside of any regulatory limitation. More discretion means the stablecoin is more likely to fit the relevant tests for securities.

C. Whether the purchaser of a stablecoin expects profits dependent on the managerial efforts of the issuer (an essential factor in the *Howey* test).[6] We note that some stablecoin issuers also offer interest on issued coins under certain conditions. Additionally, traditional stable value funds are regulated as securities despite offering no profits or growth beyond mere wealth preservation. An expectation of profits would augur in favor of the stablecoin being classified as a security.

D. Whether the stablecoin is issued alongside additional promises or services upon which the purchaser relies. In *Gary Plastic v. Merrill Lynch*, a court found that even if the underlying asset (in that case bank-issued certificates of deposit) were not securities, the purchaser agreement as a whole could be a security if additional promises were made (in that case guaranteeing a liquid market for resale before CD maturity, and managing deposit insurance claims, among others).[7] If the issuer of a stablecoin also provides a liquid market for buying and selling the stablecoin, or otherwise promises to enhance the value inherent in holding the stablecoin, then the purchaser agreements as a whole, if not the underlying stablecoin itself, could be found to constitute a securities offering.

We cannot determine with authority whether USDT or any other stablecoin is a security; that should be determined by a judge. These are, however, the primary factors that we believe will influence that determination.

---

[4] *Id.* ("we examine whether some factor such as the existence of another regulatory scheme significantly reduces the risk of the instrument, thereby rendering application of the Securities Acts unnecessary.").

[5] *Supra* note 2.

[6] *Id.*

[7] *Gary Plastic Packaging v. Merrill Lynch,* 903 F.2d 176 (2d Cir. 1990).

Regarding the second half of the question, "what are the investor protections in place for counterparty risk of insolvency in stablecoins," the answer will, again, depend on the facts of any specific stablecoin. If the stablecoin in question is issued by a US state banking authority regulated entity (*i.e.* a licensed money transmitter or a chartered trust company), then various protections will be in place including minimum capital requirements, bonding, yearly examinations, mandated consumer disclosures and other guardrails.[8] If the stablecoin is issued by an overseas entity without comparable supervision, then there may not be protections in place beyond the securities laws.

---

[8] *See*, e.g., "Organization of a Trust Company for the Limited Purpose of Exercising Fiduciary Powers," New York State Department of Financial Services, accessed September 10, 2021, https://www.dfs.ny.gov/apps_and_licensing/banks_and_trusts/procedure_certificate_merit_trust_comp.

<u>**Questions for Mr. Peter Van Valkenburgh, Director of Research, Coin Center, from Ranking Member Tom Emmer:**</u>

- **Do cryptocurrencies and/or stablecoins pose a risk to financial stability?**

Cryptocurrencies and stablecoins are fundamentally different assets so we'll take each in turn.

Cryptocurrencies do not pose a meaningful risk to financial stability. Cryptocurrencies are, speaking generally, commodities.[9] Just like more traditional physical commodities (gold, oil, etc.), cryptocurrencies are scarce, fungible, and durable goods. Just like gold or oil they can be used for various purposes or purchased on spot-markets and held as a speculative investment. As with other commodities, their value is not backed by the promises of an issuer, promoter, or other counterparty. Instead, their value is derived from basic interplay of supply and demand.

Speaking generally, financial stability is jeopardized when a significant number of investors take leveraged positions in assets with inherent information asymmetries that cause malinvestment, sudden price changes due to uncertainty, widespread bankruptcy, and ultimately contagion to the larger market. These information asymmetries are prevalent in exotic assets that are designed, backed, or insured by some issuer or authority, *e.g.* tranched mortgage backed securities, credit default swaps, collateralized debt obligations, etc. Investors may believe they have a reliable impression of the relative risks inherent in these investments but they are often unable to get a full picture of those risks because of intractable uncertainties inherent in relying on several counterparties and associated promises, *e.g.* mortgagees, insurers, and securitizers.

When an investor purchases a commodity on a spot market (including a cryptocurrency) there is no such chain of counterparties. There is no issuer or promoter whose promises about the asset could be revealed as fraudulent or ill-conceived. The prices of these assets can, without a doubt, be volatile. Gold has swung wildly in value over the past and oil prices even swung negative briefly during the substantial supply chain disruptions at the start of the novel coronavirus pandemic. Cryptocurrencies like Bitcoin and Ethereum similarly evince notorious price volatility. Nonetheless, volatility is anticipated by commodities investors. Facts about the commodities market are to a large extent public knowledge, and no promise or guarantee is ever presumed to back the value of a commodity asset. The public availability of commodities market information and the lack of reliance-generating counterparties reduces dangerous information asymmetries and limits price uncertainty. For example, even though oil prices

---

[9] "Digital Assets Primer," Commodity Futures Trading Commission, December 2020, https://www.cftc.gov/media/5476/DigitalAssetsPrimer/download.

turned negative in the summer of 2020, they quickly rebounded and the episode did not cause a wider and lasting shock to the economy writ-large.

When commodity trading becomes highly financialized (*e.g.* margin trading, leverage, securitization etc.) those commodities derivatives could, of course, begin to exhibit the same price uncertainty and contagion risk as other assets. However, that is not a problem inherent to cryptocurrencies or cryptocurrency spot market transactions; these issues are inherent in derivatives writ-large (be they cryptocurrency derivatives, or any other derivative) and that's why regulations apply to much of the derivatives trading landscape. If there is an addressable stability risk there, it comes from inadequate derivatives regulation, rather than something insidious about spot market purchases of commodities.

Several prominent economists agree that the cryptocurrency market does not pose substantial risks to financial stability. Last July, Atlanta Fed President Raphael Bostic said, "There's a lot of volatility in it, but right now it's not at a scale and it doesn't have a reach into the economy that has systemic implications for us[.] … It's not something I really incorporate very much into how I think about where our policy should be."[10] Similarly, St. Louis Federal Reserve president James Bullard has said that "By itself I don't see [it] as a systemic concern at this point," and "We are all quite aware that crypto can be very volatile."[11]

Last May the European Central Bank published a report finding that risks to financial stability from crypto assets "appear limited."[12] Additionally, a poll of leading European economists conducted by the UK based Center for Macroeconomics found that over 70% did not believe that cryptocurrencies posed any threat to financial stability.[13]

Stablecoins, unlike cryptocurrencies, are backed by an issuer or issuers. Their continued value is reliant on the promises of their issuers. This reliance can create the sort of information asymmetries discussed earlier. Accordingly, stablecoins may be a threat to financial stability if they are utilized at scale and if they are not sensibly issued and backed. We note that some stablecoins are issued by American companies that are supervised by state banking regulators. These regulations may alleviate otherwise dangerous asymmetries. Other stablecoins, however, are issued by overseas entities without comparable regulatory supervision. These may carry greater uncertainty for investors which, if their usage was at a sufficient scale, could result in larger market disruptions. However, this is an issue of enforcing existing laws and regulations

---

[10] "Fed officials: Crypto rout not a systematic concern," *Reuters*, May 19, 2021, https://www.reuters.com/technology/bullard-crypto-rout-not-systemic-concern-2021-05-19
[11] *Id.*
[12] "Financial Stability Review, May 2021," European Central Bank, May 2021, https://www.ecb.europa.eu/pub/financial-stability/fsr/html/ecb.fsr202105~757f727fe4.en.html.
[13] "Bitcoin and the City," *Center for Macroeconomics (CFM) Surveys*, Center for Economic Policy Research, December 19, 2017, https://cfmsurvey.org/surveys/bitcoin-and-city.

rather than an indictment of stablecoins as an asset type in general. As Fed Board Vice Chair for Supervision Randal Quarles has remarked, "We do not need to fear stablecoins. The Federal Reserve has traditionally supported responsible private-sector innovation. [A] global U.S. dollar stablecoin might support the role of the dollar in the global economy. And the concern that stablecoins represent the unprecedented creation of private money and thus challenge our monetary sovereignty is puzzling given that our existing system involves—indeed depends on—private firms creating money every day."[14] As Quarles continues, the issue is not private issuance of dollar backed tokens, but rather a question of finding an appropriate regulatory form for the issuer: "these concerns are eminently addressable—indeed, some stablecoins have already been structured to address them. When our concerns have been addressed, we should be saying yes to these products, rather than straining to find ways to say no."[15]

- **Blockchains have been portrayed as a way to improve digital identity and cybersecurity; are cryptocurrencies needed to achieve these benefits?**

Blockchains on their own, as in hash-linked data structures, are merely a particular way to encode information, and, as such, do little to improve digital identity and cybersecurity. By analogy, a lousy summer blockbuster won't miraculously become a great film simply because you've released it on 8K Blu-ray discs. Blockchains that are generated by cryptocurrency networks and secured by an open set of participants, however, do offer real promise to improve digital identity and cybersecurity. We call these "permissionless" or "open" blockchain networks.[16]

Traditional databases, whether for identity data or other valuable information, are only as secure as the individual or company that maintains the servers and software upon which they rely. Traditional databases have so-called root users who can view and manipulate any piece of information that the database contains. As such, if that root user account is compromised, so too are the accounts of every other user. Open blockchain networks do not have root users. The network as a whole comes to agreement over shared data, a process called consensus, and any individual user is only ever able to manipulate data that is associated with cryptographic credentials that she controls. For example, I can move bitcoins from one address to another if and only if I have a private key that corresponds to the sending address. No other person on earth can move those bitcoins unless they obtain my private key.

---

[14] Randal K. Quarles, "Parachute Pants and Central Bank Money," Speech before the 113th Annual Utah Bankers Association Convention, Sun Valley, Idaho, June 28,2021, https://www.federalreserve.gov/newsevents/speech/quarles20210628a.htm.
[15] Peter Van Valkenburgh, "Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet," *Coin Center* (2016) https://coincenter.org/entry/open-matters.
[16] *Id.*

Hacking remains an issue even with open blockchain networks because any individual user could be attacked, her keys and credentials compromised, and her valuable data stolen or cryptocurrency moved. However, in an open blockchain network there is no root user whose account could be compromised such that everyone's valuable data is placed at risk. This change in architecture and the resultant elimination of a risk-generating central party or choke point is what makes *open* blockchain networks promising innovations from an information security perspective.

Open blockchain networks cannot exist without cryptocurrencies.[17] People all over the world must be incentivized to maintain and secure these networks. If that incentive was dependent on a legal contract to pay dollars, or some other promise to pay some other traditional currency, then we'd still have a root user choke point problem of sorts: whoever makes that promise or whoever backs the value of that currency would be the single point of failure who could, in theory, be hacked and thus compromise the data of all network users. Therefore, cryptocurrency networks are deliberately designed to automatically remunerate honest participants with an asset that is described by data within the blockchain itself, a cryptocurrency. For example, persons securing the bitcoin blockchain (often referred to as bitcoin miners) can give themselves a reward denominated in bitcoins when they add a new valid block to the chain. If Bitcoin relied on bank transfers of dollars in order to reward miners for maintaining the blockchain then the system could be easily attacked by hacking the relevant banks and stopping the payments.

Permissionless blockchain networks powered by cryptocurrencies are, therefore, foundational to making meaningful improvements in digital identity technologies and cybersecurity generally. While open blockchain networks primarily record transactional data about user cryptocurrency transactions, there's no technical reason why they could not also record other socially relevant data like the issuance or revocation of an identity credential. Engineered carefully this would be a significant improvement over existing siloed digital identity systems that are only as secure as the company that maintains the centralized database. Major enterprise software developers have begun to seriously explore these tools. For example, Microsoft has worked extensively on an open source decentralized identity tool, the Ion Network, that anchors critical data in the bitcoin blockchain to ensure global availability and tamper resistance.[18]

---

[17] *Id.*

[18] Pamela Dingle, "ION– Booting up the network," *Microsoft*, June 10, 2020, https://techcommunity.microsoft.com/t5/identity-standards-blog/ion-booting-up-the-network/ba-p/1441552.