Committee on Banking, Housing, and Urban Affairs
Cryptocurrencies: What are they good for?
July 27, 2021

Angela Walch
Professor of Law, St. Mary's University School of Law
Research Associate, UCL Centre for Blockchain Technologies

Responses to Questions for the Record

UNITED STATES SENATE COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

Hearing on
Cryptocurrencies: What are they good for?
July 27, 2021

Questions for Professor Angela Walch, Professor of Law and Research Associate, St. Mary's University School of Law and UCL Centre for Blockchain, from Senator Catherine Cortez Masto:

1) **If Americans decide to hold digital tokens in significant volume, commercial banks will face a compression of margins. What mechanisms can you expect commercial banks to implement to recoup fees from consumers?**

If Americans hold digital tokens in significant volume and conduct many financial activities through them, they may engage in fewer financial activities through banks and the traditional financial system. This could result in a loss of fees by banks as they lose customers to the crypto financial system.

Actors in the traditional financial system, including commercial banks, are responding to the growth of the crypto financial system in a number of ways. First, they are seeking to integrate digital assets into the financial products they offer consumers, such as futures products and investment funds whose returns are based on the performance of digital assets. They are also building infrastructure that intersects with the crypto financial system, such as custody services to enable institutions to hold digital assets. I also expect commercial banks to offer advisory services to clients on investment strategies for digital assets, to provide research services and reports on the crypto financial system, and to invest directly in digital assets on their own behalf. Some may push to issue stablecoins, and some are becoming validators/miners within crypto systems. There are no longer sharp divisions between the traditional financial system and the crypto financial system.

2) Should we require the Financial Stability Oversight Council (FSOC) to become more involved with regulating cryptocurrencies? Does FSOC have a role to help us collaborate with other nations to prevent money laundering and crime enabled by cryptocurrencies?

FSOC may have a role to play in regulating cryptocurrencies. That is because it seeks to be a body that sits astride the fragmented financial regulatory structure we have in the US, bringing the leaders of the various financial regulatory agencies together to monitor and address threats to financial stability. The byzantine, fragmented federal financial regulatory structure has arguably hindered the US response to crypto, contributing to uncertainty about which regulatory agency should be addressing which crypto-related issues. This confusion has arguably enabled the systemic risks posed by crypto to grow while the agencies try to figure out their regulatory boundaries (as has happened in the debate over which digital assets are securities and which are commodities).

Whether it is FSOC or another task force, I believe that a unified task force is needed to determine how the US should respond to crypto, and that this is a matter of urgency. That is because the siloed regulatory agencies are in a sense imprisoned by their own regulatory mandates, which makes it difficult to think holistically about the crypto issue. My recommendation to the Committee is to create a unified task force for crypto with a diverse set of parties (including critics, proponents, and technologists) in the discussion to ensure that the recommendations of the task force are grounded in facts rather than aspirations or myths.

3) What difficulties do securities and banking regulators at the state and federal level face to prosecute fraudulent and unregistered offers and sales of digital asset securities?

There are a number of difficulties that state and federal regulators face in these prosecutions. A non-exhaustive list includes those described below.

1) Each crypto system is unique. This means that the digital assets running on that system are unique, and that each requires individual scrutiny by regulators to evaluate whether the token is a security or a commodity, or whether the token doesn't really fit neatly in either regulatory category. This requires expertise and time from the regulators. When there are new crypto systems launching all the time, it requires a lot of manpower and expertise to keep up. This is different from companies that regulators are used to that

have more standardized entity structures (e.g., corporations or LLCs) and accounting practices.

2) Each crypto system is fast-moving and evolving. At this point, there are no fully 'ossified' crypto systems, and arguably, none of them will ever be ossified, as they are complex mixtures of people (developers, miners/validators, users) and technology (cryptography and mechanism design) that may change based on the decisions made by people comprising the system. This means that regulators cannot make a decision about the status of a particular digital asset as a security or commodity (as they have done in characterizing bitcoin and ether as commodities, for example) and think that the status question is forever resolved. If the system changes (perhaps becoming more centralized in the composition of its developers or validators), it may make sense for a digital asset to be treated as a security at some points in its life and as a commodity at other points, even vacillating between the two.[1] This is an undesirable situation as it limits predictability and legal certainty for people building crypto systems and those using digital assets. It can undermine the credibility of the regulatory framework if a particular digital asset is found not to be a security, but later events mean that the digital asset should be treated as a security, and the regulator feels that it has to live with the non-security/commodity categorization for *stare decisis* reasons.

3) There remains dispute over which digital assets are securities and which are commodities. The SEC has been criticized by the crypto industry for regulating by enforcement rather than through issuing clear guidance, while the SEC has stated a number of times that it believes that the rules on what digital assets are and are not securities are clear.[2] There also appears to be somewhat of a turf war between the CFTC and the SEC over which digital assets fall in which agency's regulatory perimeter.[3] This means that there is a risk of some digital assets falling into a regulatory gap, or that consumers/investors could be

[1] For a discussion of the problems with using "decentralization" as a standard for evaluating whether a token is a security or a commodity, see Angela Walch, D*econstructing 'Decentralization': Exploring the Core Claim of Crypto Systems,* in CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES (Oxford Univ. Press, ed. Chris Brummer, 2019). For other explorations of decentralization as a legal standard, see Josh Garcia and Jenny Leung, *Data Points to Measure Blockchain Network Centralization*, Oct. 2020, available at https://ketsal.com/blog/quantifying-blockchain-network-centralization/; Gabriel Shapiro, *Defining Decentralization for Law*, April 2020, available at https://lex-node.medium.com/defining-decentralization-for-law-58ca54e18b2a.

[2] *See, e.g.,* Laurie Dunn, *SEC rules on crypto are just not clear*, Bitcoin Insider, Sept. 15, 2021.

[3] *See* Nikhilesh De, *State of Crypto: SEC vs. CFTC*, CoinDesk (Op-Ed) (Aug. 31, 2021).

harmed during the period that the agencies are figuring out which of them should address a particular activity or digital asset.

4) Limited staff and funding is also a hindrance to prosecution, particularly given the exploding scale of the crypto financial system and its rapid intermingling with the traditional financial system.[4] The SEC has formed a Strategic Hub for Innovation and Financial Technology (FinHub) and the CFTC a "Lab CFTC" to focus on financial technology innovations, among them digital assets, but it is likely that hiring additional staff to address digital assets would enhance the agencies' efforts in this area.

4) Should every digital payment service cooperate in all law enforcement initiatives, including, but not limited to, anti-money laundering requirements, Know Your Customer, and anti-trafficking projects?

This is a difficult question for policy makers to sort through. If one is confident that the existing anti-money laundering regulatory framework is effective in stopping money laundering, the financing of terrorism, and human trafficking, and that it provides the right balance of privacy and deterrence of crime, without causing other harms such as excluding people from financial system, then it makes sense to apply the framework to equivalent risks and activities in crypto. FATF and FinCEN have been working to extend the existing AML/KYC framework, though there is significant debate as to which parties in the crypto financial system should have responsibilities akin to banks to police AML on behalf of the government.

There are two issues important to think through regarding AML and crypto. First, the existing AML framework relies on banks to assist law enforcement in policing money laundering, in large part due to the intermediary role they play in financial transactions. Crypto proponents argue that applying the AML framework from the banking world to them does not make sense because crypto transactions are not intermediated, but direct from person to person, meaning that there is no party within crypto transactions for AML rules to target. I believe that this is inaccurate, given the middleman role that miners/validators play in every crypto transaction. Miners are arguably a

[4] *See e.g.*, Gary Gensler, Chair of the SEC, Written Testimony before the Senate Committee on Banking, Housing, & Urban Affairs, Sept. 14, 2021 ("As our capital markets have grown, though, the SEC has not grown to meet the needs of the 2020s. At the end of fiscal year 2016, the SEC had 4,650 people on board. Nearly five years later, though, that number had decreased by about 4 percent.").

regulatory intervention point for addressing AML goals, though they have been excluded from the AML regulatory perimeter by FATF and FinCEN thus far.

The second issue related to AML and crypto is that crypto proponents, along with others, have raised important concerns about the existing AML regulatory framework. These include concerns about privacy and whether the government should have visibility into every financial transaction people engage in, along with the cost/benefit ratio of the existing AML framework (how much money laundering/crime does it stop compared to the costs of implementation, limits on financial freedom, and excluding people from the financial system). Concerns about government surveillance and financial privacy are among the reasons that people are attracted to crypto, and flag that it may be time to reevaluate the policy goals of the existing AML framework, and whether the way Congress is achieving those goals strikes the right balance in terms of privacy, crime prevention, regulatory burdens, and financial inclusion.

5) Should we be worried that, if widely adopted, cryptocurrencies will substantially limit the ability of countries to use capital controls in times of financial crisis?

Without commenting on the merits of capital controls, I believe that this is a realistic worry unless gateways to obtaining cryptocurrencies (such as exchanges or crypto ATMs) were also targeted by the capital controls.[5] If people hold cryptocurrencies for themselves, it is harder for capital controls to reach them because they are not participating in the traditional banking system. If citizens of a country perceive that a financial crisis is brewing and capital controls may shortly be imposed, they may choose to purchase cryptocurrencies in advance of capital controls to remain in control of their value.

[5] *See* Maggie R. Hu, Adrian D. Lee, & Talis J. Putnins, *Capital Flight: Evidence from the Bitcoin Blockchain*, available at https://www.efmaefm.org/0EFMAMEETINGS/EFMA%20ANNUAL%20MEETINGS/2020-Dublin/papers/EFMA%202020_stage-1301_question-Full%20Paper_id-338.pdf (Draft of Jan. 15, 2020) (examining the use of bitcoin to evade Chinese capital controls); Yang Yu and Jinyuan Zhang, *Flight to Bitcoin*, available at https://ssrn.com/abstract=3278469) (2020) (examining a possible 'flight to bitcoin' by citizens in countries with heightened economic uncertainty); Jill Carlson, *Cryptocurrency and Capital Controls*, available at https://ssrn.com/abstract=3046954 (2016) (examining the use of bitcoin by Argentinians to evade capital controls).

Committee on Banking, Housing, and Urban Affairs
Cryptocurrencies: What are they good for?
July 27, 2021

Questions for Professor Angela Walch, Professor of Law and Research Associate, St. Mary's University School of Law and UCL Centre for Blockchain, from Senator Kyrsten Sinema:

1) Cybersecurity remains a growing concern in both the public and private sectors. Do you believe that the use of cryptocurrencies and blockchain technology has the potential to mitigate cyber threats to institutions in both the public and private sectors through the use of alternative methods of file storage, direct transactions, and other use-cases for cryptocurrencies?

Cryptocurrencies and blockchain technologies are often referred to as inherently secure and robust to cybersecurity threats. Despite this reputation, there have been many successful attacks on various crypto systems and there are various attack vectors that exist.[6] It is important to recognize that parties *within* crypto systems, such as the miners/validators and software developers, also pose attack risks to the system, much as 'insider' attacks pose cybersecurity risks in non-blockchain systems.[7] Though crypto systems are generally described as fully open and transparent, without concentrations of power that could be exploited, these are overstatements and can cause us to miss opportunities for exploitation by insiders. For example, in September 2021, there was a 'supply chain attack' on the software code for an application for SushiSwap, a decentralized exchange that operates on Ethereum.[8] A 'supply chain attack' is one in which a developer intentionally embeds code that could be exploited (in this case, to steal funds, though the funds ended up being returned). Further there have been numerous bugs in the software code of various blockchains and blockchain applications that have been exploited, or that were fixed on emergency bases through the sometimes non-public actions of small groups of software developers and miners.[9]

---

[6] For an overview of known possible attacks on blockchain systems, see Tobias Guggenberger, Vincent Schlatt, Jonathan Schmid, and Nils Urbach, *A Structured Overview of Attacks on Blockchain Systems*, Twenty-fifth Pacific Asia Conference on Information Systems, Dubai, UAE (2021) (identifying 87 known types of attacks on blockchain systems); Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang, and Aziz Mohaisen, *Exploring the Attack Surface of Blockchain: A Systematic Overview,* https://arxiv.org/pdf/1904.03487.pdf (2019).

[7] *See* Ivan Homoliak, Flavio Toffalini, Juan Guarnizo, Yuval Elovici, and Martín Ochoa, *Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures,* ACM Computing Surveys, Vol. 52, Issue 2, pp. 1-40 (2019).

[8] *See* Ax Sharma, *Cryptocurrency launchpad hit by $3 million supply chain attack*, ArsTechnica, Sept. 17, 2021.

[9] For a discussion of several of these, s*ee* Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains* in REGULATING BLOCKCHAIN. TECHNO-SOCIAL AND LEGAL CHALLENGES, (eds Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos & Stefan Eich), Oxford University Press, 2019; Angela Walch, D*econstructing*

Further, viewing cryptocurrency transactions as 'direct' or 'peer to peer' is problematic as they are intermediated by miners and validators within the crypto systems. Miners and validators are able to exploit their powers of selecting and ordering transactions to be added to the blockchain, and it is an open research question as to whether this issue can be resolved.

2) There have been multiple instances of cryptocurrencies being used for the purposes of money laundering and threat financing. How can Congress best mitigate the risk posed by bad actors' use of cryptocurrencies while enabling consumers and institutions in both the public and private sectors to benefit from the use of such new and emerging technologies?

This is a difficult question for policy makers to sort through. If one is confident that the existing anti-money laundering regulatory framework is effective in stopping money laundering, the financing of terrorism, and human trafficking, and that it provides the right balance of privacy and deterrence of crime, without causing other harms such as excluding people from financial system, then it makes sense to apply the framework to equivalent risks and activities in crypto. FATF and FinCEN have been working to extend the existing AML/KYC framework, though there is significant debate as to which parties in the crypto financial system should have responsibilities akin to banks to police AML on behalf of the government.

There are two issues important to think through regarding AML and crypto. First, the existing AML framework relies on banks to assist law enforcement in policing money laundering, in large part due to the intermediary role they play in financial transactions. Crypto proponents argue that applying the AML framework from the banking world to them does not make sense because crypto transactions are not intermediated, but direct from person to person, meaning that there is no party within crypto transactions for AML rules to target. I believe that this is inaccurate, given the middleman role that miners/validators play in every crypto transaction. Miners are arguably a regulatory intervention point for addressing AML goals, though they have been excluded from the AML regulatory perimeter by FATF and FinCEN thus far.

'Decentralization': Exploring the Core Claim of Crypto Systems, in CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES (Oxford Univ. Press, ed. Chris Brummer, 2019);

The second issue related to AML and crypto is that crypto proponents, along with others, have raised important concerns about the existing AML regulatory framework. These include concerns about privacy and whether the government should have visibility into every financial transaction people engage in, along with the cost/benefit ratio of the existing AML framework (how much money laundering/crime does it stop compared to the costs of implementation, limits on financial freedom, and excluding people from the financial system). Concerns about government surveillance and financial privacy are among the reasons that people are attracted to crypto, and flag that it may be time to reevaluate the policy goals of the existing AML framework, and whether the way Congress is achieving those goals strikes the right balance in terms of privacy, crime prevention, regulatory burdens, and financial inclusion.

3) The conversation around central bank digital currencies (CBDCs) has grown in recent years. Chairman Powell has stated that the Fed awaits authorization from Congress before moving forward with the development and implementation of a US CBDC. Would a blockchain-based US CBDC benefit consumers by better protecting financial transactions? Are there additional benefits or risks associated with the use of blockchain technology for the purposes of a US CBDC?

Global research into CBDCs is looking broadly into many possible technology implementations, including blockchain-based systems.[10] Although cryptocurrencies (which are blockchain systems) were arguably what stimulated central banks to consider CBDCs, it is important to consider whether a blockchain technology-based CBDC offers benefits over other possible technologies. There are two different types of blockchain technologies that could be used: public/permissionless blockchains or private/permissioned blockchains (sometimes referred to as distributed ledger technologies, or DLT). Researchers have largely ruled out using public/permissionless blockchains for CBDCs, but DLT is still part of the research discussion.

[1010] See, e.g., Sarah Allen et al., *Design Choices for Central Bank Digital Currency*, GLOBAL ECONOMY & DEVELOPMENT WORKING PAPER 140 | July 2020, available at https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf; David Chaum, Christian Grothoff, Thomas Moser, *How to issue a central bank digital currency*, SNB Working Papers (March 2021), available at https://www.snb.ch/n/mmr/reference/working_paper_2021_03/source/working_paper_2021_03.n.pdf; Raphael Auer & Rainer Böhme, *The Technology of retail central bank digital currency*, BIS Quarterly Review, pp. 85-96 (Mar. 2020).

With reference to public/permissionless blockchains (such as Bitcoin, Ethereum, and other cryptoeconomic systems on which cryptocurrencies run), a critical difference between a CBDC and a cryptocurrency is that a CBDC is offered by a central issuer (the central bank) and the success of that CBDC will depend on trust in the central bank and the applicable country, along with the technology used to build the CBDC. By contrast, with a cryptocurrency, there is no single central issuer of the applicable token, as many parties within the blockchain system work together to issue and maintain the token.

A public/permissionless system like that used with Bitcoin or Ethereum is a poor fit for a CBDC because there is no accountability to the public (as would be required for a government currency), and because the central bank would not be able to control the monetary (or other) policies of the CBDC. Thus, adopting a cryptocurrency as legal tender, as El Salvador has recently done, poses risks to consumers (e.g., volatility, operational risks) that the government or central bank cannot easily mitigate.[11]

With regard to DLT-based CBDCs, there is debate about whether DLT is necessary or worthwhile. Some argue that using DLT-based systems introduces unnecessary complexity and reduced efficiency (including in transaction processing capacity) to the system without corresponding benefits in resilience or privacy.[12] Others, like Sweden, are trialing CBDCs using permissioned blockchain systems.[13] This is a matter of ongoing research and debate, however, with complex technical, policy, and legal considerations involved, and there are no easy or settled answers at this time.

---

[11] See Tobias Adrian and Rhoda Weeks-Brown, *Cryptoassets as National Currency? A Step too Far*, IMF Blog, July 26, 2021 (discussing the risks raised by El Salvador's designation of Bitcoin as legal tender).

[12] See, e.g., David Chaum, Christian Grothoff, Thomas Moser, *How to issue a central bank digital currency*, SNB Working Papers (March 2021), available at https://www.snb.ch/n/mmr/reference/working_paper_2021_03/source/working_paper_2021_03.n.pdf (proposing a CBDC that does not use blockchain technology).

[13] Sveriges Riksbank, *E-krona pilot: Phase 1,* April 2021, available at https://www.riksbank.se/globalassets/media/rapporter/e-krona/2021/e-krona-pilot-phase-1.pdf (reporting on the results of the trial of e-krona using a blockchain-based system, and on the need for further research for this new technology).