## **Testimony before the**

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

Hearing on

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

#### **Introduction**

Thank you Chairman Brown, Ranking Member Toomey, and members of the Committee, for the opportunity to testify today.

My name is Angela Walch. I am a Professor of Law at St. Mary's University School of Law in San Antonio, Texas, and a Research Associate at the Centre for Blockchain Technologies at University College London. At St. Mary's, I teach courses in Contracts and Philosophy of Law, along with a course on blockchain technologies and the law and a seminar on the Law of Money.

I have been studying cryptocurrencies since 2013, when I first taught about Bitcoin in my Law of Money course. My research has focused on the governance of crypto systems, the problematic use of language in the crypto space, and the ways misunderstandings about these systems can contribute to systemic risk.<sup>1</sup> Because my research deals with foundational questions

<sup>&</sup>lt;sup>1</sup> My research is available on the Social Science Research Network (SSRN) or at www.angelawalch.com. Representative works include Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk,* 18 NYU Journal of Legislation & Public Policy 837 (2015); Angela Walch, *Open Source Operational Risk: Should Public Blockchains Serve as Financial Market Infrastructures?* in HANDBOOK OF BLOCKCHAIN, DIGITAL FINANCE, AND INCLUSION, VOL. 2 (Elsevier, David Lee Kuo Chuen and Robert Deng, eds., 2017); Angela Walch, *The Path of the Blockchain Lexicon (and the Law)* 36 Review of Banking & Financial Law 713 (2017); 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, *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, in CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES (Oxford Univ. Press, ed. Chris Brummer, 2019); Angela Walch, *Crypto Miners as Intermediaries* (in progress).

at the heart of this new field, it intersects with many of the fields that come together in crypto systems, including law, economics, computer science, archival studies, philosophy, and others. I would describe my research as "Crypto Realism" as it takes a critical approach to these systems, their uses, and their impacts on society. I believe it is essential to take a critical, realistic approach to these systems due to their potential to impact large numbers of people in important ways.

Given the explosive growth of a separate crypto financial system over the last decade, and the immaturity of academic and public understanding in this area, I am in the process of developing a multidisciplinary Center on Digital Assets and Society at St. Mary's, with the goal of facilitating urgently needed multidisciplinary research in this field, providing a convening site for discussion and learning, and contributing to a grounded, realistic understanding of how these systems operate and impact society.

I am happy to be able to discuss these important issues with the Committee today, as I consider it vital that policy makers have a realistic (rather than idealistic) understanding of the crypto financial system. Please note that given the constraints of the hearing, the discussion of the topics I cover in my testimony is necessarily high-level and incomplete, but I have tried to provide a useful starting point for discussion.

In my written testimony, I address five areas, as requested by the Committee:

- In Part 1, I provide definitions and explanations of key terms and concepts around cryptocurrencies, including a high-level view of their governance structures and use of cryptoeconomics (predictions of how humans respond to incentives) to incentivize parties to maintain and protect the systems;
- 2) In Part 2, I describe the functions and uses of cryptocurrencies;
- 3) In Part 3, I discuss the extent to which cryptocurrencies are integrated within or linked to the traditional financial system;
- 4) In Part 4, I discuss the social and financial costs and benefits of cryptocurrency, as well as risks that cryptocurrencies pose to the U.S. financial system, investors, consumers, and other participants in the economy; and
- 5) In Part 5, I close by discussing how flaws in academic, industry, and public understanding of cryptocurrencies (i.e., idealistic rather than realistic understanding) can taint policy and risk decisions, embedding risk to be revealed when reality bites.

Please note that the views I express in my written and oral testimony are my own, and not those of any organizations with which I am affiliated. I do not own any cryptocurrencies, and I

have no financial interests in the crypto financial system. I have previously received summer research funding from St. Mary's University School of Law, where I teach.

### I. <u>Key Terms and Concepts</u>

The terminology used in the crypto space has been challenging since Bitcoin's inception.<sup>2</sup> Vocabulary fluctuates quickly, and terms are contested virtually all the time, as the field itself is fast-moving and conceptual boundaries are porous. As I will discuss further below, this unsettled language contributes to confusion and misunderstandings about the crypto financial system, which makes policy makers' jobs more difficult and embeds risk.

Nevertheless, I will attempt to define a few key terms and concepts to assist our conversation. For purposes of this hearing, the conceptual division of cryptocurrencies, crypto tokens, and digital assets into different buckets (laid out by Goldman Sachs in a recent newsletter)<sup>3</sup> is consistent with how I use these terms and how I see others using them in the crypto space. Note that while I agree with Goldman Sachs' conceptual division, I do not fully agree with the precise definitions it provides, so will provide my own where indicated. Please note that there is no definitively established definition of any of these terms.

*Cryptocurrency*: A native, manmade representation of value whose movements are tracked on a blockchain record within a cryptoeconomic system. Examples of cryptocurrencies include bitcoin and ether.

*Cryptoeconomic System:* A sociotechnical system comprised of different groups of people that is designed to use peer-to-peer computer networks, cryptography, and predictions about how humans respond to incentives to create a record of the movements of its native cryptocurrency.<sup>4</sup> [Note that I will use the term "crypto systems" as shorthand for "cryptoeconomic systems" in this testimony.]

*Crypto Tokens:* A digital asset "created by platforms that build on top of other blockchains. For example, the tokens of Uniswap and Aave— UNI and AAVE—are built on the Ethereum network." They are distinguished from cryptocurrencies which are native to a cryptoeconomic system. "Tokens can be used not only as mediums of exchange or stores of value, but also for governance decisions (e.g. voting on changes or upgrades to the protocol) or to access platform services."<sup>5</sup>

<sup>&</sup>lt;sup>2</sup> See, e.g., Angela Walch, *The Path of the Blockchain Lexicon (and the Law)*, 36 Review of Banking & Financial Law 713 (2017); Angela Walch, *Blockchain's Treacherous Vocabulary: One More Challenge for Regulators*, 21 No. 2 Journal of Internet Law 1 (2017).

<sup>&</sup>lt;sup>3</sup> Goldman Sach's recent research newsletter *Crypto: A New Asset Class?*, May 21, 2021 (https://www.goldmansachs.com/insights/pages/crypto-a-new-asset-class-f/report.pdf).

<sup>&</sup>lt;sup>4</sup> See Shermin Voshmgir & Michael Zargham, Foundations of Cryptoeconomic Systems, available at <u>https://assets.pubpub.org/sy02t720/31581340240758.pdf</u>, for an in-depth discussion of this concept. The study of cryptoeconomic systems is considered a new multidisciplinary field of research.

<sup>&</sup>lt;sup>5</sup> This definition is slightly revised from Goldman Sachs' definition of "crypto tokens."

*Digital Assets: "*An intangible asset created, traded, and stored digitally. Digital assets in the crypto ecosystem include cryptocurrencies and crypto tokens."<sup>6</sup>

These definitions do not attempt to cover all characteristics of cryptocurrencies, cryptoeconomic systems, crypto tokens, or digital assets, as the characteristics themselves remain poorly understood and disputed. They are intended, however, to provide grounding for our conversation.

*Governance:* The committee also requested testimony on the governance structures of cryptocurrencies. I will provide some high level commentary on the topic, but note that this is an entire field of study on its own that is in its infancy. At a very high level, governance of cryptocurrencies deals with questions like what goes into the software that the network of computers runs, what transactions end up on the blockchain record and the order they appear, how changes are made to the software run by the network, and how changes are made to the underlying protocol (the ruleset of the network). Parties that are involved in the governance of crypto systems include software developers, miners (sometimes called validators or record keepers), and other stakeholders like users, token holders, or big players in the ecosystem like crypto exchanges.

In my view, the governance of crypto systems is critical to understand – who has power, how may it be exercised, and what are the limits of power? Since crypto systems emerged with Bitcoin, a dominant thread of the conversation about them has been that they are "decentralized," and therefore lack sites of meaningful power. You may have heard that in crypto systems, you don't have to trust humans and their fallible, corrupt natures – you just have to trust math. If I have one message for the Committee today, it is that this statement is just inaccurate. Cryptoeconomic systems remain subject to human flaws and corruption, whether in how the software is coded, whether the game theory designed to operate the system is robust, or whether miners collude to exploit their power to order transactions in the blockchain record to their benefit. Since Bitcoin's 2009 launch, events across the crypto ecosystem have demonstrated time and again that parties *within* crypto systems (not just those intermediaries *outside* the systems like exchanges or wallet providers) exercise meaningful power. You may find many examples of these exercises of power in my research.<sup>7</sup>

It is also important to note that the crypto financial system is characterized by experimental governance. New governance techniques, voting mechanics, and forums are being iterated on in all parts of the crypto ecosystem. I do not critique the innovation efforts here, but it is important

<sup>&</sup>lt;sup>6</sup> This is Goldman Sachs' definition of "digital assets."

<sup>&</sup>lt;sup>7</sup> 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, *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, in CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES (Oxford Univ. Press, ed. Chris Brummer, 2019); Angela Walch, *Crypto Miners as Intermediaries* (in progress).

to consider the consequences of real-time experimentation on the governance of multibillion dollar systems with increasing linkages to the traditional financial system.

#### II. <u>Functions and Practical Uses of Digital Assets</u>

Digital assets (including crypto tokens and cryptocurrencies) are used for a variety of purposes, which I believe my fellow witnesses, as representatives of the crypto industry, will be able to provide information on.

At a high level, digital assets and the crypto financial system serve many of the same purposes as the traditional financial system – it is just different people performing the tasks in sometimes different (and sometimes the same) ways.

Some examples of how people are using digital assets include:

- as a way of increasing or preserving wealth (the 'store of value' use case);
- to make payments (e.g., remittances);
- as a hedge against a loss in value of other assets, such as US dollars or other assets in one's wealth portfolio;
- as a way of escaping financial surveillance;
- to enable protest against authoritarian governments;
- to participate in economic activities in the crypto ecosystem, such as the purchase of NFTs (non-fungible tokens that are being used for digital works of art, for example) or digital file storage space;
- as collateral for obtaining loans.

Though cryptocurrencies are not widely accepted as a form of payment, many believe this use will increase, with some speculating that Amazon may soon accept bitcoin as a payment method.<sup>8</sup> Further, El Salvador has now adopted legislation making bitcoin a legal tender there, and there is speculation that other countries may soon follow. And in DeFi (short for "decentralized finance"), the financial system being built on top of the Ethereum network, financial products mirroring those in the traditional financial system are rapidly being created, as well as new ones.

At this point, I think the crypto space has developed and continues to develop in a way that it will soon be fair to describe it as an alternative full-fledged financial system, if it is not already.

III. Integration with Traditional Financial System

<sup>&</sup>lt;sup>8</sup> Matt Novak, *Amazon Rumored to Accept Bitcoin By End of 2021 and Develop Own Currency by 2022: Report*, Gizmodo, July 26, 2021 (https://gizmodo.com/amazon-to-accept-bitcoin-by-end-of-2021-and-develop-own-1847360405).

Cryptocurrencies began as niche communities after Bitcoin's launch in 2009. The early users of Bitcoin, for example, were largely people who were interested in the system as an innovative new technology, or who were drawn to it ideologically due to its separation from the traditional financial system (no banks) or the monetary policy it embedded (i.e., its "cap" of 21 million bitcoins).<sup>9</sup>

Around 2015-2016, institutions in the traditional financial system became enamored of the "blockchain technology" that Bitcoin and other cryptocurrencies operate on. There was an explosion of interest in permissioned blockchains or "DLT" (distributed ledger technology), with participation in the group record-keeping process governed by explicit contractual obligations rather than by game theory. These permissioned systems had the goal of harnessing the technological innovation of crypto systems, while jettisoning their permissionless wildness. Proponents of permissionless systems argued that the permissioned blockchains were basically joint venture databases, missing out on the true innovation of permissionless blockchains.

Since 2017, however, there has been increasing interest and investment from the traditional financial system in permissionless crypto systems like Bitcoin, Ethereum, and others. The "snowball effect" is a good way to think about the integration of digital assets into the traditional financial system, starting out very small, and then building on earlier integrations to grow ever more rapidly. Government responses to the COVID pandemic (e.g., large relief packages) appear to have accelerated the trend.<sup>10</sup> Here are just a few examples of the ways that digital assets are being integrated into or linked to the traditional financial system:

- Widespread investment by institutional investors in digital assets.<sup>11</sup>
- Traditional financial institutions offer crypto custody services.<sup>12</sup>
- Growing use of stablecoins like Tether and USDC from Circle.
- Major investments by venture capital firms into crypto and the crypto ecosystem.<sup>13</sup>

<sup>&</sup>lt;sup>9</sup> I put "cap" in quotation marks to indicate that there is no fixed technical barrier that limits bitcoin to 21 million coins. The 21 million limit is currently supported by the Bitcoin community, but the community has the choice to alter the limit in the future. There have been proposals by prominent Bitcoin community members to consider changing the 21 million cap, as it is uncertain how the system will function once new bitcoins are no longer awarded to miners, and the miners must rely solely on transaction fees to maintain the blockchain. However, there is definitely a strong norm within the Bitcoin community to keep the 21 million limit.

<sup>&</sup>lt;sup>10</sup> For an overview of institutional involvement in digital assets, see Goldman Sach's recent research newsletter *Crypto: A New Asset Class?*, May 21, 2021 (https://www.goldmansachs.com/insights/pages/crypto-a-new-asset-class-f/report.pdf).

<sup>&</sup>lt;sup>11</sup> Anna Irrera, *Most Institutional Investors Expect to Buy Digital Assets, Study Finds,* Reuters, July 19, 2021 (reporting on Fidelity Digital Assets' 2021 survey of institutional investors that finds 7 in 10 institutional investors expect to buy or invest in digital assets in the future, and that more than half of institutional investors in Asia, Europe, and the US currently invest in digital assets).

<sup>&</sup>lt;sup>12</sup> E.g., Fidelity, Gemini, Coinbase, and others offer this service.

<sup>&</sup>lt;sup>13</sup> Brandon Kochkodin, *Venture Capital Makes a Record \$17 Billion Bet on Crypto World*, Bloomberg, June 18, 2021; Kate Rooney, *Andreessen Horowitz launches \$2.2 billion crypto fund and is 'radically optimistic' despite price fluctuations*, CNBC, June 24, 2021.

- Direct ownership of cryptocurrencies such as Bitcoin by companies like Square, Microstrategy, and Tesla.<sup>14</sup>
- Companies providing crypto services (e.g., exchanges, Bitcoin mining) are now publicly traded.<sup>15</sup>
- Bitcoin and Ethereum futures have been trading for several years now.
- Major institutions are offering access to crypto funds to their clients.<sup>16</sup>

With financial media like Bloomberg and CNBC talking about crypto virtually around the clock, and topics like "Bitcoin" or "crypto" regularly trending on Twitter, the trajectory is definitely towards ever-increasing integration of crypto into the traditional financial system.

Aside from direct institutional investment, other recent crypto events increase its potential to impact the traditional financial system and the broader economy. Examples include the June announcement that El Salvador is making bitcoin a legal tender<sup>17</sup> and the rapid influx of bitcoin miners to places like Texas following China's crackdown on bitcoin mining earlier this year.<sup>18</sup>

#### IV. Social Impact and Risks

The story of crypto is complex, offering both benefits and risks to society and the economy.

#### Benefits

Proponents argue that crypto systems provide an alternative means of governance and economic freedom outside of existing institutions. This means more than just having an alternative to big banks within the traditional financial system. Using crypto (particularly a cryptocurrency that enables one to transact anonymously (such as Zcash or Monero)) is also a way of hedging against a surveillance state or even a collapsing state. There is something to the argument that financial privacy is important, and that important freedoms are lost if every single expenditure of value may be viewed (and perhaps censored) by the state or another powerful intermediary.<sup>19</sup> We see this same argument playing out as central banks evaluate the level of privacy that central bank digital currencies should have and whether cash should be eliminated.

<sup>&</sup>lt;sup>14</sup> Stephen Graves and Daniel Phelps, *The Ten Public Companies with the Biggest Bitcoin Portfolios*, Decrypt, July 16, 2021 (https://decrypt.co/47061/public-companies-biggest-bitcoin-portfolios).

<sup>&</sup>lt;sup>15</sup> For example, Coinbase, a US-based crypto exchange went public in April 2021, and several Bitcoin mining companies are publicly traded (e.g., Marathon Digital and Riot Blockchain).

<sup>&</sup>lt;sup>16</sup> Emily Mason, *About-Face: JPMorgan Opens Crypto Trading to All Clients*, Forbes, July 22, 2021.

<sup>&</sup>lt;sup>17</sup> Nelson Renteria, Tom Wilson, and Karin Strohecker, *In a world first, El Salvador makes bitcoin legal tender*, Reuters, June 9, 2021.

<sup>&</sup>lt;sup>18</sup> David Pan, Why China's Ban on Crypto Mining is More Serious than Before, CoinDesk, July 9, 2021; Dalvin Brown, *Bitcoin miners break new ground in Texas, a state hailed as the new cryptocurrency capital*, The Washington Post, July 8, 2021.

<sup>&</sup>lt;sup>19</sup> See Jerry Brito, *The Cash for Electronic Cash*, Coin Center Report, Feb. 2019 (https://www.coincenter.org/the-case-for-electronic-cash/).

In authoritarian regimes around the world, we have seen governments use control over the payment system to crack down on dissent, so this concern is not invalid.<sup>20</sup>

Crypto proponents use terms like "censorship resistant" and "permissionless" to describe the benefits of crypto systems, stating that any two parties in the world are able to send and receive value directly – without going through or having to seek permission from an intermediary. If I were a dissident in an authoritarian country, I could see how this would be a lifeline. However, I believe that crypto proponents are overstating (perhaps innocently) the censorship-resistance of existing systems, and that they may not provide as much freedom as some hope, given the power of miners in the system to manipulate the ordering of transactions or delay them. In Section V below, I talk about how mainstream understanding about fundamental characteristics of crypto systems is inaccurate, and how those inaccuracies serve as sites of hidden risk.

Crypto proponents also claim that the costs of engaging in financial transactions are lower than in the traditional financial system, and that more people are able to participate in finance and better themselves because they do not have to pass through gates like accredited investor evaluations. This may be true, but my sense is that costs are lower largely because crypto systems are generally unregulated at the moment. Traditional financial institutions could lower their costs to consumers if they had fewer regulatory costs, and I'm sure they would be happy to have additional customers for their financial products. Regulatory avoidance appears to be source of lower costs and broader participation – Congress may wish to reevaluate existing regulations, but the policy drivers of protecting consumers in financial transactions remain, whether in the crypto financial system or the traditional financial system.

#### Costs and Risks

Cryptocurrencies and other digital assets do pose significant risks currently, and the risks they pose increase as they permeate the traditional financial system and more and more people invest. The financialization we have seen of cryptocurrencies and crypto tokens means that a problem in a single cryptocurrency (such as, for example, a software bug that causes the Ethereum network to fork (or split)) could ripple through all the financial products tied to that cryptocurrency, as well as all investors in the cryptocurrency, and companies that provide other services and products related to the cryptocurrency. Further, since many investors appear to view digital assets as an asset class, a flaw in a flagship cryptocurrency like bitcoin or ether could drag the rest of the digital asset markets down as well. Although we have not yet seen ripple effects from the extreme price movements that seem endemic to digital assets, we cannot rule out such effects in the future, particularly as they become more widely used and more integrated into the traditional financial system.

With the currently unregulated nature of cryptocurrencies, their experimental governance systems, which lack the formalized accountability structures of the traditional

<sup>&</sup>lt;sup>20</sup> See Alex Gladstein, *Bitcoin is Protecting Human Rights Around the World*, Reason, Feb. 5, 2021 (https://reason.com/video/2021/02/05/bitcoin-is-protecting-human-rights-around-the-world/).

financial system, can be sites of risk. It is critical to recognize crypto systems like Bitcoin and Ethereum as infrastructure, as they support the cryptocurrencies themselves, as well as any products or activities built on top of the systems. This means that the governance of the infrastructure is incredibly consequential, as we have learned in my home state of Texas with the failures of our electrical grid infrastructure during the February 2021 winter storm. In short, governance of infrastructure matters to those who rely on it, even if they don't realize it.

As mentioned earlier, the governance of crypto systems includes the software developers within them, as well as the validators/miners of transactions, along with users. It is still a matter of heated debate as to how much power any of these groups has.

Drilling down a bit, the software developers of systems like Bitcoin and Ethereum generally use the governance methods of grassroots open source software to write and propose changes to the code.<sup>21</sup> This means that they have no obligation to take care of the code for the benefit of those who rely on it, and they have no duty not to exploit their privileged positions for their own benefit. With large companies like Square now funding several Bitcoin developers, it will be important to acknowledge the conflicts of interest inherent in the relationship, and to ensure that the small group of software developers who run these financial infrastructures know where their duties run. For this reason, I have analogized the key software developers of systems like Bitcoin and Ethereum to fiduciaries, as large numbers of people depend on them to be both competent and to act in the best interest of the system.<sup>22</sup> I note that this theory has been subject to much debate.<sup>23</sup>

Miners or validators are also part of the governance of crypto systems, and are similarly infrastructure providers to all who rely on the operation of that system. Miners select, order, and propose transactions to be added to the blockchain record. While many characterized crypto systems as lacking intermediaries and enabling the direct transfer of value between transacting parties, that is technically untrue.<sup>24</sup> Transactions do not appear on the blockchain record unless a miner chooses to put them on. While the transaction selection and ordering power was generally overlooked as a meaningful power for many years, in the past several years, the exploitation of the transaction ordering power has become a major issue. Termed "MEV" or "Miner Extractable Value", the amounts that miners are able to "extract" from users wanting to use the blockchain demonstrates the importance of this power and the falsity of the

<sup>&</sup>lt;sup>21</sup> Angela Walch, *Open Source Operational Risk: Should Public Blockchains Serve as Financial Market Infrastructures?* in HANDBOOK OF BLOCKCHAIN, DIGITAL FINANCE, AND INCLUSION, VOL. 2 (Elsevier, David Lee Kuo Chuen and Robert Deng, eds., 2017).

<sup>&</sup>lt;sup>22</sup> 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.

<sup>&</sup>lt;sup>23</sup> See, e.g., Raina Haque et al, *Blockchain Development and Fiduciary Duty*, Stanford Journal of Blockchain Law and Policy (2019); Gabriel

<sup>&</sup>lt;sup>24</sup> Seen Angela Walch, Crypto Miners as Intermediaries (in progress); Antony Lewis, Bitcoin's Payments Are Not Peer to Peer!, BITS ON BLOCKS (Dec. 3, 2018), https://bitsonblocks.net/2018/12/03/bitcoins-payments-not-peer-to-peer/; PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN & THE LAW (2018), 180 (describing miners or other transaction processors as intermediaries supporting blockchain-based networks).

"disintermediation" narrative.<sup>25</sup> A full discussion of MEV and the powers of miners is beyond the scope of this testimony, but it is a site of active discussion and research in the crypto space.

I highlight these parties (developers and miners) because they have largely been left out of the policy and risk discussion, due to mainstream views of cryptocurrencies and crypto tokens as "things" like commodities. From my perspective digital assets are highly malleable, subject to the actions of parties like developers, miners, and other participants in the applicable crypto system, and failing to take their malleable nature into account is a source of risk.

Finally, there is also more research needed on the environmental costs of the proof of work mechanisms used in mining Bitcoin and Ethereum, as there is debate on this matter.

I also note that there are many more ways digital assets and crypto systems pose risks to society, but my discussion is limited to those I have focused on in my own research.

#### V. <u>Realism vs Idealism</u>

I will close by emphasizing that crypto systems are very new, experimental, and poorly understood. The knowledge infrastructure around these systems is shaky and has lots of errors built into it. Many of the "facts" that we "know" about crypto systems are simply wrong, and making decisions based on idealized versions of crypto systems instead of the realities embeds risk in every decision that is made. Based on my work in the field since 2013, using any of the following words in an absolute sense to describe a crypto system is problematic, yet highly consequential decisions are being based on these beliefs every day:

- Immutable
- Decentralized
- Trustless
- Enables direct transfers of value
- Secure
- Tamper-proof
- Disintermediated
- Open/Transparent
- Neutral
- Embody philosophies that can't be changed

I recommend that if you see these words used in a policy paper or academic piece in an "absolute" versus a "relative" way, that you take the analysis you are provided with a grain of salt, or come talk to me about it.

<sup>&</sup>lt;sup>25</sup> See Philip Daian et al., *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*, arXiv:1904.05234v1 (April 10, 2019), available at https://arxiv.org/pdf/1904.05234.pdf

More research into these systems is desperately needed, and it is unfortunate that we seem to have again put the cart before the horse by building massive systems atop poorly understood infrastructures. I urge Congress to fund research in this area, to ensure diversity of perspectives on any task forces that it creates to examine these issues (including academics who are not part of industry), and to recognize how consequential these systems are for our world today – for better or for worse.

Thank you again for the opportunity to testify, and I look forward to your questions.