S. HRG. 117–578

CRYPTOCURRENCIES: WHAT ARE THEY GOOD FOR?

HEARING

BEFORE THE

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

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

ON

EXAMINING THE PROBLEMS AND POSSIBILITIES OF CRYPTOCURRENCY

JULY 27, 2021

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: https://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
50–802 PDF WASHINGTON : 2023

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

SHERROD BROWN, Ohio, *Chairman*

JACK REED, Rhode Island
ROBERT MENENDEZ, New Jersey
JON TESTER, Montana
MARK R. WARNER, Virginia
ELIZABETH WARREN, Massachusetts
CHRIS VAN HOLLEN, Maryland
CATHERINE CORTEZ MASTO, Nevada
TINA SMITH, Minnesota
KYRSTEN SINEMA, Arizona
JON OSSOFF, Georgia
RAPHAEL WARNOCK, Georgia

PATRICK J. TOOMEY, Pennsylvania
RICHARD C. SHELBY, Alabama
MIKE CRAPO, Idaho
TIM SCOTT, South Carolina
MIKE ROUNDS, South Dakota
THOM TILLIS, North Carolina
JOHN KENNEDY, Louisiana
BILL HAGERTY, Tennessee
CYNTHIA LUMMIS, Wyoming
JERRY MORAN, Kansas
KEVIN CRAMER, North Dakota
STEVE DAINES, Montana

LAURA SWANSON, *Staff Director*
BRAD GRANTZ, *Republican Staff Director*

ELISHA TUKU, *Chief Counsel*
TANYA OTSUKA, *Counsel*
COREY FRAYER, *Professional Staff Member*

DAN SULLIVAN, *Republican Chief Counsel*
LANDON ZINDA, *Republican Counsel*

CAMERON RICKER, *Chief Clerk*
SHELVIN SIMMONS, *IT Director*
CHARLES J. MOFFAT, *Hearing Clerk*

C O N T E N T S

TUESDAY, JULY 27, 2021

WITNESSES

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

CRYPTOCURRENCIES: WHAT ARE THEY GOOD FOR?

TUESDAY, JULY 27, 2021

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 10 o'clock a.m., via Webex and in room 538, Dirksen Senate Office Building, Hon. Sherrod Brown, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN SHERROD BROWN

Chairman BROWN. The Senate Committee on Banking, Housing, and Urban Affairs will come to order.

First, I would like to take a moment to acknowledge the passing of our friend and former colleague, Senator Mike Enzi. Some of us served with him on this Committee, which he joined in 1997. We remember his kindness, his personal birthday notes that we all looked forward to. He spoke at our Ohio College Presidents Conference each year—we always try to bring in leaders of both parties—sharing his insights about higher education with higher education leaders in my State. He talked often of bipartisanship, and he meant it.

On a personal note, I think of our long discussions about Boy Scouts. We were both Eagle Scouts, and we often talked about his life's work, really, in many ways, to strengthen the scouting movement. Our thoughts are with his wife Diana, his children Amy, Emily, and Brad, and with the people of Wyoming. A true public servant.

Since Bitcoin came online in 2009, thousands of these so-called "digital assets"—virtual currencies, cryptocurrencies, stablecoins, investment tokens—have poured into the markets. All of these currencies have one thing in common: they are not real dollars. They are not backed by the full faith and credit of the United States. And that means they all put Americans' hard-earned money at risk. From tech giants like Facebook's Libra—or Diem, or however their PR consultants attempt to rebrand it next—to fly-by-night operations, we have seen far more empty promises than we have seen viable cryptocurrencies.

A cottage industry of decentralized financial schemes has also cropped up alongside these alternative financial products, in the hopes of creating a parallel financial system with no rules, no oversight, and no limits. They claim to enable "transparency." Their backers talk about the "democratization of banking." There is noth-

ing "democratic" or "transparent" about a shady, diffuse network of online funny money.

After a decade of experience with these technologies, it seems safe to say that the vast majority have not been good for anyone but their creators. This technology is almost never used to buy goods and services, which is what any currency is supposed to be used for, after all. Some cryptocurrency supporters see these technologies as a way to take power back from the Wall Street bankers, whose too-often complicated and opaque financial scheming crashed the economy.

When the only other option appears to be Wall Street, maybe it is hard to blame anyone for putting their faith in cryptocurrency. I hear the same message—we all do—over and over from people in our States that they do not trust banks, and they especially do not trust the biggest banks. They have been burned over and over again by fees, by minimum balances, by waiting periods, by segregated "second chance" accounts. And of course, they all remember the crash, the bailouts, the lack of accountability. But as these technologies have developed, most of them seem to mirror, rather than to challenge, the Wall Street model.

In fact, traditional financial institutions are angling to become the biggest players in these markets, and it is a good bet they will find even more creative ways to use these new technologies to dodge accountability and put our entire economy at risk again.

We should all be concerned. Thankfully, President Biden has begun to replace Trump-era financial appointees with real financial watchdogs, who take seriously the job of protecting people's hard-earned money. But the financial recovery remains fragile, as coronavirus variants emerge, and there are still regulators to appoint. Yes, some of these underlying technologies may have useful applications, beyond evasion of banking and securities laws. These are generally applications outside of finance. One of those technologies we will hear about today, Filecoin, uses economic incentives to provide digital storage space.

But if we want a solution to Americans' legitimate fears and concerns and anger about our financial system, shady startups are not the answer. We need more community banks that are actually in people's neighborhoods and that understand their lives. We need No-Fee Accounts, backed by the full faith and credit of the United States through the Federal Reserve, that allow everyone to open a bank account and make online purchases. And we need to show people there will be accountability, not just a default to the same Wall Street system where bankers get all the profits and working families get all the risk.

We need to make sure the American economy remains the safest and most dependable in the world. The last thing we should be doing is giving another industry a chance at wrecking that reputation, a reputation our entire economy depends on.

The best thing we can do to protect Americans' money is to adopt smart regulations that protect consumers, that protect investors, that separate the innovators from the extortionists. I look forward to learning more from our witnesses today.

Ranking Member Toomey.

OPENING STATEMENT OF SENATOR PATRICK J. TOOMEY

Senator TOOMEY. Thank you, Mr. Chairman. One sentiment that I certainly share with you were your kind remarks about our former colleague, Mike Enzi. I do not know if I have met a more good, decent, honorable man than Mike Enzi. We are going to miss him, and our hearts go out to his lovely wife, Diana.

Today's hearing provides us an opportunity to learn about the current and potential uses of cryptocurrencies. In short, a cryptocurrency connects one person with another through open, public networks, separate from Government control or any other intermediaries. And cryptocurrencies are a growing part of our economy. The first cryptocurrency, Bitcoin, was implemented in 2009. And while there are varying definitions of what is considered a cryptocurrency, there are now thousands of them available in many different forms.

According to a recent University of Chicago survey, 13 percent of Americans bought or traded cryptocurrency in the past 12 months. That is more than half of the total percentage of Americans who invested in stocks during that same period of time.

Like other currencies, cryptocurrencies may be useful as a store of value or a medium of exchange. However, it is important to acknowledge up front that a significant impediment to cryptocurrencies, or at least most cryptocurrencies, becoming a widely used store of value or medium of exchange is their price volatility. That problem could potentially be solved by tying a cryptocurrency to other assets, such as a fiat currency like the U.S. dollar, for instance. And that is what are meant to do.

On the other hand, some cryptocurrencies may prove to be useful as a store of value by serving as alternatives to fiat currencies, like the dollar. They may serve as a store of value because, unlike fiat currencies, the Government cannot come along and print trillions of a cryptocurrency. In this way, cryptocurrencies might complement the role that gold has historically played as a store of value and hedge against inflation. For example, we have seen recently in Venezuela how people can use Bitcoin to store value when a Government devalues its currency.

Also, some cryptocurrencies may prove to be useful as a medium of exchange for buying goods and services. With cryptocurrencies, making payments and conducting transactions may become cheaper, easier, and faster for consumers than it is using traditional currencies. Cryptocurrencies can be exchanged without the need for an intermediary, such as a bank, which could virtually reduce transaction costs and fees for consumers to zero. In addition, since a person does not need a bank account to use cryptocurrencies, they could increase access to financial services for many Americans.

Beyond these often-discussed uses for cryptocurrencies, there are other ways that the distributed ledger technology that underlies crypto can be used. A distributed ledger is a data base that shares information across various sites and geographies that is accessible by multiple people. This structure ensures that all of these people can access and verify the data, and it dramatically reduces the risk of any one central actor manipulating the data. In my view, the use of distributed ledger technology to have nonintermediated transactions verified in a foolproof way is a very powerful technological

innovation, and this innovation already is having an impact on supply chains, financial services, and securing digital identities.

And it has significant potential for verifying the ownership of property, whether it might be automobiles, homes, or securities. In the United States, we spend a lot of time and money to verify property ownership. Distributed ledger technology may provide a way to do this faster and at a lower cost.

Over time, it is possible that the application of this innovation may become more important than the usefulness of crypto as a currency per se, and we are already seeing it have a real world impact. As we know, democracy and individual freedom in Hong Kong are under assault from the Chinese Communist Party. That assault has included the forced closure of a prodemocracy newspaper, *Apple Daily*. But the Chinese Government has not been able to erase *Apple Daily*'s important work. That is because R-weave, a cryptocurrency network that enables permanent data storage, was used to permanently store portions of the paper. This technology makes it impossible for the Chinese Government to destroy *Apple Daily*'s work, no matter how hard it tries. That is just one example.

Today we will hear from two expert witnesses about other current and potential uses of cryptocurrencies. Mr. Jerry Brito is Executive Director of Coin Center, a think tank focused on cryptocurrencies and related topics. He will discuss an array of uses for cryptocurrencies and how these technologies could be further developed. Ms. Marta Belcher is Chair of the Filecoin Foundation. She helped to develop and launch a cryptocurrency, Filecoin, that provides data storage access on a decentralized file storage network.

Now it is important to note that many people have raised legitimate issues about cryptocurrencies. These include their use in illicit activity and their possible effects on monetary policy and on our existing financial infrastructure. I think we need to discuss and understand these issues, and address them if we need to. But we should not lose sight of the tremendous potential benefits that distributed ledger technology offers. We should also be mindful that private innovation has enabled most of these developments. We should not suppress the concepts of individual entrepreneurship and empowerment that have made this innovation possible.

I look forward to hearing from our witnesses today about the ways cryptocurrencies are impacting and can potentially impact our lives, and I hope we will listen with open minds.

Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Toomey.

Our witnesses today are Professor Angela Walch, Professor of Law, St. Mary's University School of Law, Research Associate at the University College London Centre for Blockchain Technologies. Welcome, Professor Walch.

Mr. Jerry Brito, Executive Director of Coin Center, a nonprofit research and advocacy organization focused on policy relating to cryptocurrencies and other distributed computing technologies. Welcome, Mr. Brito.

And Ms. Marta Belcher, Chair of the Filecoin Foundation. She is also the General Counsel and Head of Policy at Protocol Labs, and

she is counsel to the Electronic Frontier Foundation. Welcome, Ms. Belcher.

Professor Walch, you are recognized for 5 minutes.

Thank you for joining us.

STATEMENT OF ANGELA WALCH, PROFESSOR OF LAW, ST. MARY'S UNIVERSITY SCHOOL OF LAW, RESEARCH ASSOCIATE, UCL CENTRE FOR BLOCKCHAIN TECHNOLOGIES

Ms. WALCH. Thank you. Chair Brown, Ranking Member Toomey, and Members of the Committee, good morning and thank you for inviting me to testify here 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.

I have been researching cryptocurrencies since 2013, and have published numerous papers on the topic. My research is focused on the governance of cryptosystems, the problematic use of language in the cryptospace, and the ways that misunderstandings about these systems can contribute to systemic risk.

I have a few key messages for the Committee today. First, over the past several years, we have witnessed the creation of an alternative cryptofinancial system, with the growth of this financial system dramatically increasing over just the past year or two. Cryptocurrencies hit a market cap of over $2 trillion in April, and there has been rapid integration of digital assets into the traditional financial system through investments by large, publicly traded companies and venture capital firms, the creation of cryptobased financial products, and the building of infrastructure to enable both retail and institutional investors to participate more seamlessly in the cryptoecosystem. Each of these actions creates links between the cryptofinancial system and the traditional financial system.

Second, as the cryptofinancial system grows and more links are created between it and the traditional financial system, there is potential for crises in the cryptofinancial system to cross over to the traditional financial system, causing a systemic crisis. This could result in widespread harm to the public, both in the U.S. and globally, including to people who have not chosen to invest or otherwise participate in the cryptofinancial system.

As a single example, imagine a critical software bug in a cryptocurrency like Ether, causing the Ethereum network to split in two, creating uncertainty and panic amongst Ether holders and the entire decentralized financial system that runs on the Ethereum network, known as DeFi. With enough links between the cryptofinancial system and the traditional financial system, such a crisis could ripple through those links to the traditional financial system, spreading the effects of this single software bug widely.

Third, many of the decisions that we are making about the cryptofinancial system appear to be based on idealized views of crypto rather than realistic views. Another way to say this is that people and institutions may be investing in crypto's, promise and policymakers and regulators may be making decisions about how to treat the cryptofinancial system, based on myths about crypto.

Let me give you a few examples. You have probably heard that cryptosystems like Bitcoin and Ethereum are transformational and

positive for freedom because they are decentralized and have no intermediaries, and therefore no intermediary risk; that they enable people to send value directly over the internet, just like you might pay someone in cash; that they create immutable records that cannot be changed; that certain ones, like Bitcoin, have fixed caps on the number of units that can ever be created; that they are secure and tamper-proof, open and transparent, so no bad behavior can be hidden; that they are protected and regulated internally by the incentives built into the systems; that concentrations of power that could be exploited do not exist or are sufficiently checked by the design of the system.

If all of this were indisputably true, then yes, this does sound amazing and like something everyone should be participating in. But every single one of these "characteristics" of cryptocurrencies and digital assets that I have recited is only sort of true, as each requires an asterisk to indicate the many limitations on its accuracy. If you analyze these systems carefully, you realize that what are claimed to be characteristics of these systems are largely aspirations of these systems. Treating aspirations as reality means that every single decision based on the aspirations is flawed and embeds risk. If we believe that cryptosystems have no intermediaries, for example, and make investment and regulatory decisions based on this fact, then the intermediaries that do exist can exploit their positions with impunity, as we are seeing with miners on the Ethereum network today.

No one thinks the existing financial system is perfect. It is riddled with problems, corruption, concentration of power, exploitation, excessive risk-taking, and other human problems that Congress has long sought to contain and remedy through regulation. But crypto, understood through a realistic lens, is not a miracle, "get out of the financial system free" card. It has the same problems. We need to acknowledge the power concentrations within it and make thoughtful policy and risk decisions about how to address that power.

Thank you again for inviting me, and I look forward to your questions.

Chairman BROWN. Thank you, Professor Walch. Mr. Brito, you are recognized for 5 minutes. Thank you for joining us.

STATEMENT OF JERRY BRITO, EXECUTIVE DIRECTOR, COIN CENTER

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

The title of this hearing is "Cryptocurrencies: What Are They Good For?" After a decade since Bitcoin's invention, what do we have to show for it? What justifies all the hype and investment? Is there today any tangible use case that is meaningfully improving people's lives?

Those questions bring to mind the early days of another open, permissionless network, the internet. There was real skepticism that despite all the hype over the information superhighway we still have very little to show for it, leading Paul Krugman to famously predict, in 1998, that, quote, "The growth of the internet

will slow drastically because most people have nothing to say to each other. By 2005 or so, it will become clear that the internet's impact on the economy has been no greater than the fax machines," end quote.

The fact that in 1998, there was no Wikipedia or Netflix or Zoom could lead one to believe that there never would be and that the internet would continue to only be the domain of its earliest adopters—computer enthusiasts, spammers, gamblers, and pornographers. What skeptics missed is that an open and permissionless platform, to which anyone could connect and on which anyone could build, would allow an explosion of entrepreneurial innovation that would give us applications we could not imagine or predict. Cryptocurrency networks like Bitcoin are open and permissionless networks just the same. And while we may not yet have the Wikipedia or Netflix of cryptocurrency, that does not mean that we never will. And indeed, there are thousands of entrepreneurs around the world developing new applications of cryptocurrency networks, some of which I have no doubt will change the world, even if I cannot now predict what they are.

But even if we cannot predict the future, what are some concrete applications that we can see today? First, there is the base application of Bitcoin, permissionless, person-to-person payments. In the U.S., we take for granted that we can send each other funds effortlessly with our smartphones, but this is not the case everywhere in the world, especially where authoritarian Governments block payments to and from dissidents. Just last year, prodemocracy labor activists in Belarus and antipolice violence protesters in Nigeria successfully turned to the Bitcoin network to accept donations because local banks would not bank them.

Beyond payments and money, I would point to novel applications of cryptocurrency's tamper-resistant ledgers. Chinese social media is heavily censored. This has led Chinese activists to post messages to the Ethereum blockchain where they cannot be taken down. There are many applications of cryptocurrency networks being developed for free speech that cannot be censored by authoritarian Governments.

Perhaps more relevant to average Americans are the potential applications of cryptocurrency and its tamper-resistance to enable identity solutions for cybersecurity. The root cause of many data breaches, such as those of Experian, Equifax, or OPM, is the fact that if an attacker can compromise the password of one individual, he may gain access to the personal information of millions of others. Microsoft is a company that is painfully aware of this vulnerability, as it provides the identity infrastructure for over 90 percent of the Fortune 500 companies.

This is why Microsoft spent years helping develop a decentralized identity standard built on top of Bitcoin. It is called the ION network. It was launched in March. It is live and operational, and is now a candidate web standard. By replacing usernames and passwords with decentralized identifiers, the ION network will allow individuals to control their own identities rather than trust data brokers that can be compromised at root. This means that an attacker would no longer be able to compromise just one credential

in order to gain access to everyone else's, but would, instead, have to hack each individual, a massive improvement to cybersecurity.

Other benefits of decentralized identifiers include the ability to verify credentials, helping, for example, to combat disinformation. With ION, it will be trivially easy to verify that a photo that you are looking at was signed as authentic by his photographer, who, in turn, is credentialed by the Associated Press. Additionally, because you own your own identity and network of relationships to other identities, we will be able to see the emergence of an open, portable social graph that will allow for competition with incumbent social media networks.

All of this requires Bitcoin to work. Like the early internet, there are real, live use cases of cryptocurrency networks today, but we can only see glimpses of the truly world-changing applications to come. The Clinton administration successfully pursued a deliberate policy of avoiding undue restrictions of the internet. To reap the benefits of cryptocurrency networks I hope we have the wisdom to do the same today. Thank you.

Chairman BROWN. Thank you, Mr. Brito. Ms. Belcher, thank you for joining us here. You are recognized for 5 minutes.

STATEMENT OF MARTA BELCHER, CHAIR, FILECOIN FOUNDATION

Ms. BELCHER. Thank you, Chairman Brown, Ranking Member Toomey, and Committee Members for inviting to testify today. I am Marta Belcher. I serve as the Chair of the Filecoin Foundation, one of many companies working on a cryptocurrency called Filecoin.

The question posed by the hearing today is, "What Are Cryptocurrencies Good For?" Our answer to that question is that cryptocurrency can be the foundation for a better internet, an alternative to big tech that puts people in control of their own data, protects user privacy and security, and permanently preserves humanity's most important information. Today, I would like to explain how.

Cryptocurrency makes it possible to send monetary value across the globe instantly and securely, just as easily as you can send information over the internet by attaching a file to an email. That is to say, cryptocurrency does for monetary value what the internet did for information.

For me, the most important thing about cryptocurrency is that it creates the ability to program money. In other words, you can write computer code that automatically transfers value upon a condition being met. For example, you could write a computer program that says, for every second of a song that I play, automatically transfer the equivalent of a millionth of a cent from me to the songwriter. This can happen instantly and automatically, with no intermediary between us, even across borders. This kind of transaction would be untenable using traditional payment systems.

The cryptocurrency technology I work on, Filecoin, uses that same programmable money concept to create a decentralized file storage network. If you have extra storage space on your computer hardware, you can "rent it out" to others who will pay you to store their files (or pieces of their files, so that only the file owner can put the pieces back together. A computer program will regularly

check that the files are still being stored on your computer and, if so, will automatically compensate you with cryptocurrency. It is like Airbnb for file storage: storage providers rent out their extra storage space to earn Filecoin, and users spend Filecoin to store their files on other people's computers.

That may sound like a niche use case, but we believe this could be a foundational technology for the next generation of the internet. Today's internet is centralized. The vast majority of data making up the many websites Americans use every day sits in data warehouses owned by just three companies: Amazon Web Services, Microsoft, and Google Cloud. We have repeatedly seen these companies suffer blackouts, and vast swaths of the Web go down for hours, including websites that are massive contributors to the American economy. That is the problem with having single points of failure.

We believe you can create a better version of the Web if you combine the storage capacity and computing power on all of our individual devices into a supercomputer-like network, and store multiple copies of data across those devices. On this decentralized version of the internet, websites will stay up even if some nodes fail, and the availability of information is not dependent on any one server or company. This provides a more robust platform for humanity's most important information.

Filecoin provides the incentive for people to contribute storage to that decentralized internet. And these incentives work. Since launching last October, nearly 3,000 Filecoin storage providers have contributed nearly 8 exabytes of storage capacity. To put that in perspective, that could store all of the written works of mankind in all languages from the beginning of recorded history to today, 10 times over. And that storage space is being used to preserve humanity's most important information. As just one example, the Starling Lab, a project of Stanford and USC, uses the Filecoin network to permanently preserve the USC Shoah Foundation's archive of 55,000 video testimoneys of genocide survivors.

Filecoin is just one use of cryptocurrency, but it demonstrates how being able to program money, to instantly and automatically send microtransactions across the world, can create economic incentives that enable entirely new technologies.

There are already thousands of projects building other cryptocurrency applications, from automatically paying music royalties, to compensating people when their data is used, to paying journalists for each view of an article, to incentivizing consumers to use renewable energy. Some may not succeed, but others may move technology forward in ways we cannot yet begin to imagine.

This technology is in its early days, and this stage of development for cryptocurrency is often compared to the internet of the early 1990s. It would have been a mistake, in 1995, to believe that we understood then what the internet was good for. I would urge the Committee to embrace the possibility that cryptocurrency's uses might be just as expansive, and to ensure that innovation in this space can continue to thrive.

I look forward to your questions. Thank you.

Chairman BROWN. Thank you, Ms. Belcher.

Professor Walch, let us start with a couple of questions. Proponents of cryptocurrencies like Bitcoin or Ether use the word "decentralized"—we have all heard that word in the testimony—to make it appear that there are not companies with outsized power over these financial systems. They claim that decentralization puts users on equal footing and reduces inequality. We now know that Wall Street, megabanks, and hedge funds have a stranglehold, of course, over the financial system.

Are there similar actors who could get outsized power in cryptomarkets?

Ms. WALCH. Absolutely, yes. I think the term "decentralized" can really be misleading to us. If we stop at the label of "decentralized," because this is just crypto and that is the way it is, then we miss looking into these systems and seeing the concentrated pockets of power within them. And parties who sit in those pockets of power include the core software developers that create these systems, maintain them, are responsible for continuing to help them operate if a critical bug is discovered, making decisions about what policies are implemented into the software code that comprises the system. We have seen this again and again when there have been critical bugs identified in cryptosystems, and the four or five software developers have to make a decision about how to handle it, for the multibillion-dollar system. We also see miners in these systems having concentrations of power.

Chairman BROWN. So explore a little bit more the term "decentralized." Have there been instances where powerful companies or individuals have been able to bend the rules, claiming decentralization, but bend the rules to benefit themselves?

Ms. WALCH. So we see miners in systems like Ethereum and Bitcoin, the ones that use the proof of work consensus mechanism, being able to exploit their positions. So there are very large mining pools, and what is significant about miners is that they have a power that has not been very well understood, and that is they get to pick the transactions that are in the memory pool and decide whether a transaction goes in there, what order it goes in on this powerful ledger, and they are able to accept bribes—you can call them bribes, or you can just call them payments—to exploit that ordering power, taking money for themselves, potentially. It is called miner-extractable value. And I hope that we will be able to discuss it further, because it is seen as a potentially killer for the idea of cryptocurrencies.

Chairman BROWN. This sounds to me like something we see in this Committee on a number of different issues, sort of phony populist marketing brought to us by people that have immense power in the marketplace, one way or the other.

Let me ask you one more question, Professor. As you said in your testimony, cryptoeconomic systems are beginning to mirror the functions of the traditional financial system. Talk about risk to financial stability from having a separate financial system operating parallel to the traditional financial system. You talked in your testimony about sort of migrating into the traditional system. Delineate those risks, if you would.

Ms. WALCH. Sure. So when we have two systems sitting beside each other, one cryptofinancial system and one traditional financial

system, and one, the traditional financial system, being regulated while the crypto one is not, we can see, through these links that are being built, such as investments in cryptocurrencies by large players in the traditional financial system, like MicroStrategy, like Tesla, who are always in the news these days, with the significant institutional investments, with the cryptoinvestment products, hedge funds, venture capital funds, et cetera.

Many, many links are being formed so that things that go wrong in the cryptosystem—a catastrophic software bug, any sort of failure there—can actually have an impact on every single holder of the cryptocurrency that is affected, all the holders of financial products that embed that cryptocurrency, all the investment funds that touch that cryptocurrency, all the potential other cryptocurrencies within the cryptofinancial system, because of the fear of contagion, and that can easily ripple over to the financial system.

I am not claiming that that can happen today, but with every link that is built, and the larger the cryptofinancial system grows, that risk increases.

Chairman BROWN. Thank you. Senator Lummis is recognized for 5 minutes, from Wyoming.

Senator LUMMIS. Thank you, Mr. Chairman and Ranking Member, for allowing me to go ahead so I can go to the floor and pay a little tribute to my dear friend, Mike Enzi, that you both served with, and so many of you served with, who passed away today. And I am deeply grateful for this opportunity, so thank you.

Professor Walch, you mentioned, in your written testimony, that there are no definitively established definitions in the digital asset space, and I think you hit the nail on the head there. If we can have a law textbook like this one on virtual currency we should be able to agree on common terms.

So why is it so important that Congress and our regulators begin to use the same legal terms to talk about these issues?

Ms. WALCH. Sure. So I have thought a lot about this, and it has been an important part of my research. I think that these problems with terminology come from the fact that these systems are extremely fast moving, that there are products and activities created in the cryptofinancial system that kind of mirror the financial systems, but we do not know what to call them. Do you call them the same thing? How are they different? So there is a ton of confusion.

And we have seen this already reflected in laws that have been passed in a bunch of State legislatures, about cryptocurrencies, cryptosystem, where misunderstandings and improper terminology is embedded into the definitions in the laws that are meant to, you know, support or enable innovation with cryptocurrencies.

And I wish there was an easy solution to this problem. We have been talking about it for years, and the language, people keep adding new terms, like miner-extractable value and yield farming and a whole bunch of things that everyone has to learn anew when they come into the system. So it is a persistent problem and can have important impacts.

Senator LUMMIS. Thank you, Professor, and I do think that that is a point where Congress can weigh in. So I am looking forward to working on that through our Financial Innovation Caucus, and

perhaps bringing something forward, definition-wise, for us all to consider.

Mr.—is it Britto or Brito?

Mr. BRITO. Brito.

Senator LUMMIS. Well, it is lovely to have you here. Thank you so much. Can you give me some specific use cases on how virtual currency and the distributed ledger technology that underpins these assets has the potential to reduce the cost of financial transactions for everyone, and to create a more efficient financial system?

Mr. BRITO. Sure. Thank you for the question. There are any number of use cases where some function that today is happening in the financial system that depends on a centralized intermediary, could be done potentially more efficiently if the two parties who rely on that intermediary can connect, you know, one on one.

One example that simply comes to mind would be settlement and finality. So today when you want to trade securities or other assets you ultimately rely on a series of intermediaries that ultimately have one settlement intermediary, where there is a book that is, you know, sort of updated by that one party. You can imagine a system that depends on one global ledger, that anybody has access to, and can swap.

You know, Senator Toomey mentioned property registries. There is a potential there. So today in the United States we have title insurance. Why do we have title insurance? Well, we have title insurance because the chain of title to a piece of property might have been corrupted somewhere along the way. With cryptographic distributed ledgers the potential for that is greatly, greatly reduced. And so, for example, you might be able to eliminate the need for that kind of insurance.

Senator LUMMIS. Well, that is helpful and informative, because I would note that the St. Louis Fed has noted that the U.S. financial sector cost 8.2 percent of GDP in 2021, and that payments cost around 1 percent of GDP. Additionally, billions of dollars in capital is trapped every day because of antiquated means of payment that take days, or even weeks to settle. For a Fortune 500 company that regularly sends international wire transfers, this is costly, and it is a very big deal, and it is something that we also might be able to take advantage of by some of these new distributed ledger technologies.

Mr. Brito, we hear a lot, both true and false, about how our existing financial system benefits some groups more than others. Isn't the transparency and openness of open source finance a huge benefit that can ensure a level play field, promote financial inclusion, and create trust in our financial system?

Mr. BRITO. So I fear overpromising when it comes to saying that something like the coin or cryptocurrencies like it will guarantee financial inclusion for everybody. I think there is a lot of work that needs to be done there. But what I can say is that because these systems are broadly transparent you can see where the power centers may be, and you can go and address them, and you can see what the transactions are, and that is a great improvement. And to the extent that you can have parties interacting with each other

and doing so transparently, that would reduce the need for trust, as you say.

Senator LUMMIS. Well, one of the points you raised also sort of segues into my next question, and that is about virtual currencies and money-laundering. There is a myth that virtual currency is anonymous, but are not most virtual currency transactions recorded on a publicly available ledger that cannot be easily altered? It seems to me any criminal would avoid creating evidence like that.

Mr. BRITO. Yes. The vast majority of transactions using cryptocurrency are recorded transparently on open ledger, and these are available to law enforcement. And indeed, talking to law enforcement, they tell us how useful that evidence is. So why do criminals continue to use these networks? Well, because Bitcoin and things like it are good for payments, are good for censorship-resistant payments, and so they abuse these networks.

But you are right. They create a trail that, with the help of on-ramps and off-ramps that are regulated and compliant, it can help law enforcement find and prosecute these criminals.

Senator LUMMIS. I thank the witnesses today for their very helpful testimony, and, Mr. Chairman, I yield back with my thanks.

Chairman BROWN. Thank you, Senator Lummis. Senator Reed of Rhode Island is recognized.

Senator REED. Well, thank you very much, Mr. Chairman. Let me begin by recognizing the passing of Mike Enzi. Mike and I came to the Senate in 1997, and to this Committee in 1997, and he was a paragon of integrity and decency that we all looked up to, and his passing is deeply grieved by all of us.

With that, let me direct a question to Ms. Walch. Chairman Brown talked about the intermediaries as not simply a neutral sort of technical aspect, but they have a position which they could exploit in this system. And at this point we have no way to confirm who these people are. Is that correct?

Ms. WALCH. So I am interpreting your question to be asking about who the intermediaries are within the systems, right, who the middlemen are between one person sending a cryptotoken to another person, and that is the miners. The transaction does not end up on the blockchain unless a miner puts it on there.

So they have not yet been recognized as intermediaries. People still call these systems disintermediated. And the power that they exercise is in choosing the transactions, ordering them, and they can delay people's transactions, they can take money to do what are called things like sandwich attacks and front-running and back-running, and all kinds of games.

And there has not been very good research into the mining or validating community. They are coming out of the shadows much more. Many of them have migrated just recently from China, where they were highly concentrated, and China recently made it illegal for Bitcoin miners to operate there, so many are coming to the U.S., many to my home State of Texas.

And I think these players need more scrutiny. They are intermediaries in important multimillion-dollar, multibillion-dollar financial systems. They need more scrutiny.

Senator REED. And your question raises another question I have. China is taking a very close look at this whole operation, as indicated by their dispersion of the miners in China. What is their goal? Do they want to set up an alternate system? Do they want to be able to influence this system so that, at a critical moment, they can cause disruption?

Ms. WALCH. So I wish I could tell you what China's goal is.

Senator REED. I wish I could tell you also.

Ms. WALCH. But I think that there is speculation that China and other Nations feel threatened by cryptocurrencies, because they are alternative, nonsovereign monetary systems and financial systems, and are not easily controllable by Governments, or regulated by Governments. I mean, over the past 10 years that has been the case.

I think that China also is looking into, very strongly, issuing a central bank digital currency right now, and may feel that the threat from cryptocurrencies is more than they want to deal with, and certainly not that they want to support as much as they were within their own borders.

Senator REED. One of the other aspects, of course, and I think everyone has alluded to it, is one of the mainstays of our economic policy is macroeconomic policy, the Federal Reserve's control in the United States and the European Union system of the value of currency. And that could be compromised, either intentionally or unintentionally, by cryptocurrencies. Is that accurate?

Ms. WALCH. So, I mean, one of the original motivations of cryptocurrencies was creating an alternate financial system, an alternate monetary system, and that was due to a lack of faith, really, in existing monetary systems and a feeling that Governments were not very responsible stewards of the money that they issued.

I think there is a fundamental tension between the existence of cryptocurrencies and sovereign currencies. We are seeing that play out in very strange ways right now. I think we are in the midst of kind of a revolution and significant change on what money is and who gets to make it. We are seeing that with events like El Salvador adopting Bitcoin as legal tender. We are seeing this with the race of countries to consider whether they should issue central bank digital currencies, I think in part to compete with cryptocurrencies. And I think that given what we have seen over the past few years, with the loss of faith in institutions, which is like literally across the board, that cryptocurrencies are seen as kind of like a safety valve for collapse of important systems. So there is a lot going on here.

Senator REED. Just a comment. You know, the most incisive comment I ever heard about new, disruptive technologies is it makes good things better and bad things worse, and I think that is where we are. And that is the role of Government, to make sure the good things are preserved and the bad things are avoided. And I think the comparison is interesting, because from my perspective they have displaced newspapers, responsible reporting on TV, et cetera. We are into a world of disinformation, which is complicating our lives. Just look at the vaccination issues. And disinformation seems to be the coin of the realm now, not facts.

So I think we have to be very, very careful going forward and learn from our internet experience and think carefully about judicious ways we can provide control. Thank you.

Chairman BROWN. Thank you, Senator Reed. Senator Toomey is recognized for 5 minutes.

Senator TOOMEY. Thank you, Mr. Chairman.

Mr. Brito, Ms. Walch, in her testimony, suggests, I think it is fair to say, that it is problematic to think of some of the attributes that we often association with cryptocurrencies in absolute terms, and that they are rather relevant trends. She has got a list, you know, the idea that it is immutable, decentralized, trustless, secure, tamper-proof, disintermediated, and several others.

How do you think about this question of whether these concepts are absolute or relative, and how much does that matter?

Mr. BRITO. Sure. Thank you for the question. So I think, in any complicated system, you really cannot think in terms of absolute. When you are having conversations, perhaps even on Twitter, where a lot of these conversations happen, I think there is a shorthand to talk, you know, in a shorthand sort of way, and talk in absolutes. But I think anybody serious discussing this is not talking in terms of absolutes.

And indeed, you know—so that is certainly the case. I think it goes a little bit far to say, then, that this is confusing policymakers and regulators and people who need to pay attention to that. So if you listen to Chairman Brown's statement, clearly people are paying attention to the wiggle room here, and are addressing it.

Senator TOOMEY. Just to follow up on this, Ms. Walch also expressed the concern about problems that could emerge, bugs that could be discovered. In fact, there have been bugs discovered in cryptocurrencies. And she posited a hypothetical about, you know, a problem being discovered, say, in Ethereum, that caused a loss of confidence that cascaded into the financial system.

How concerned should we be about a problem developing in a cryptocurrency cascading into the conventional financial system?

Mr. BRITO. So I do not think it is an impossibility. It is possible. I will say two things about it. First is what is the systemic risk that exists with crypto today? And I am not an expert on systemic risk so I look to the experts. Recently, the Atlanta Fed President, Raphael Bostic, said that there is a lot of volatility but right now it is not at a scale and it does not reach into the economy in a way that has systematic implications for us. That has been echoed by St. Louis Fed President James Bullard, by the European Central Bank, et cetera, et cetera.

So we are not there. Something to keep an eye on, absolutely, and to make sure that these links that Professor Walch refers to are supervised and regulated, et cetera.

The other thing I would say briefly is a lot of what Professor Walch just said in her testimony just now is that you can have a lot of hedge funds and other investment vehicles invest in cryptocurrencies, and then later, if there is a bug, you know, could decrease in value and have systemic risk. That thing could be said for any commodity, right? Cryptocurrencies ultimately are commodities. You can imagine an investment in orange juice, and you can

imagine a literal bug that wipes out the orange crop could have systematic effect.

So it is certainly a possibility but I would not say that it is something that should lead us to shy away from cryptocurrencies, just to make sure that we have the right guard rails in place for hedge funds and other investment vehicles.

Senator TOOMEY. We have had a little discussion about miners, and miners play an essential role in validating transactions and maintaining the infrastructure. Should they be thought of as intermediaries or as people taking a bribe in return for doing the validation?

Mr. BRITO. Yeah, so I do not think it is controversial to say that miners are technically, in some broad sense, intermediaries, but I do not think they are intermediaries in the way that this Committee thinks about it. They are not financial intermediaries for financial regulation.

So for example, when I send you money using PayPal online, PayPal is clearly an intermediary, right. They are a financial intermediary that can block my transaction, not allow me to make a payment at all, can lose my money, they are a custodian, et cetera. So they are a financial intermediary, which is what we care about.

But there is another intermediary in this transaction that I am making with you, and that is my ISP, my internet service provider, right. I need my ISP as an intermediary to be able to use PayPal to pay you. But we do not think of ISPs as intermediaries, and indeed, in money transmission laws in the various States, that basically regulate the facilitation of the transmission of money, explicitly exclude ISPs and other service providers from regulation. And indeed, the New York Department of Financial Services, in their BitLicense, excludes miners, because they do not think about them as these kinds of intermediaries.

Senator TOOMEY. That is very helpful. One last question, and this is for Ms. Belcher. You discussed a fascinating, actual, real-world use case that is not about speculating on the value of the currency but rather accessing a decentralized storage.

So my question for you is, can you explain why cryptocurrency is necessary in order to deliver that service?

Ms. BELCHER. Thank you for that question, Senator. Yes. So cryptocurrency creates the incentive for people to contribute their resources, to maintain the network, and in this case to contribute file storage. And that same code that enables you to transfer money, to transfer value instantly across the internet without an intermediary, also does the process of verifying that you are, in fact, storing files.

Senator TOOMEY. Thank you. Thank you, Mr. Chairman.

Chairman BROWN. Thanks, Senator Toomey. Senator Menendez of New Jersey is recognized.

Senator MENENDEZ. Thank you, Mr. Chairman. As cryptocurrencies become more commonplace we can all agree that we will begin to see more widespread adoption of crypto as a form of payment in physical retail outlets. So I would like to ask each of you one basic question. Do you believe that a brick-and-mortar retail business, like a grocery store or a pharmacy, should be al-

lowed to accept only cryptocurrency and deny customers the opportunity to pay with cash?

Ms. BELCHER. Thank you for the question, Senator. Speaking for Filecoin, Filecoin is not intended to be a competitor to the U.S. dollar, but rather to be used for a specific purpose of file storage.

As I discussed in my testimony, cryptocurrencies have many uses beyond merely facilitating financial transactions, and I think that there are many cryptocurrencies that you can think of more like other commodities, like gold, that serve the same function without necessarily being a competitor to the U.S. dollar.

Senator MENENDEZ. Yeah. My question is rather simple. A yes or no would suffice. But I will yours as saying no. Is that——

Ms. BELCHER. Correct. The answer is no.

Mr. BRITO. Today I could open up a store and accept only euros, if I had that quirk, and I think the same should be for cryptocurrency. It is my store and it is a basic freedom.

Senator MENENDEZ. Mm-hmm. Professor.

Ms. WALCH. I have a hard time—I am a strong defender of cash, for many reasons, so it troubles me, given that not everybody has access to digital financial services that they would not be able to use cash in basic retail stores.

Senator MENENDEZ. Well, I agree with those of you who do not think it should be limited. You know, according to a May 2020 report by the Federal Reserve, over 1 in 5 Americans are unbanked or underbanked. And despite the potential, I do not think it is reasonable to expect that this segment of the population is going to suddenly jump into using cryptocurrency when they do not even have an opportunity to participate in the formal banking system.

So we need to preserve the option of choice in how you pay for retail transactions. That is why I am introducing the Payment Choice Act with Senator Cramer and others, to make sure that Americans continue to have the option of paying cash for everyday purchases, and so millions of unbanked American households are not shut out of the economy.

Let me turn to another issue, which I follow very much as the Chairman of the Foreign Relations Committee, and that is sanction evasion. I have been actively following Venezuela, Russia, and other countries' interests in developing virtual currencies for the explicit purpose of evading U.S. sanctions as well as the broader pattern of cyber criminals demanding payments in cryptocurrency from their victims. And we are increasingly seeing a confluence between these two trends.

The data firm, Chainalysis, estimates that out of all the ransomware payments made in 2020, 15 percent of them carried a risk of sanctions violations. So essentially victims of ransomware attacks are increasingly finding themselves targeted by sanctioned entities, and therefore, victims that make ransom payments in cryptocurrency may be committing sanctions violations.

So how should we, in Congress, think about addressing this problem without undermining the efficacy of our sanctions tools?

Mr. BRITO. So I will take that question, Senator. For years the FBI has been advising the victims of ransomware not pay ransom demands, and this applies to any ransom demand. And a demand

that is coming from a sanctioned party, then it is not just advice. You cannot pay the ransom.

And on the same advisory page, on their website, the FBI highlights that the way to deal with ransomware is to (a) have a good cybersecurity system to try to prevent the attack, and (b) regularly back up data and secure those backups so you can confidently refuse to pay a ransom, if it comes to that.

Ms. WALCH. I would just add one point. I think part of our vulnerabilities to ransomware that we are seeing have developed over the years with lax cybersecurity practices, and this may be tied, in part, to the liability framework that we have had around software development, which is that pretty much there is no liability even if your software is terrible and has lots of bugs, and any obligation to make good software is fully disclaimed in the software license.

So I am not saying that anyone can make perfect software, but the accountability paradigm may need to be rethought.

Senator MENENDEZ. Well, I am all for preventing the possibility of a ransomware attack, but I am not for sacrificing our sanctions ability for the essence of protecting ransomware victims.

One final question. According to the Cambridge Bitcoin Electricity Consumption Index, 4.6 percent of all Bitcoin mining occurs in Iran, making it the fifth-largest miner in the world. Because the main costs associated with mining cryptocurrency is energy, Iran is effectively able to convert its oil and natural gas reserves into cash via cryptocurrency mining.

Are there tools that would allow financial institutions and regulators to prevent the use of mining to avoid sanctions?

Mr. BRITO. Senator, while there is nothing that can prevent anyone with the right equipment and internet connection from mining, what is interesting to me about this is that Iran is turning one commodity, oil, into another commodity, and to cash, really, but into another commodity, Bitcoin, let's say. And so it still has to find a way to trade it for hard currency, which is ultimately what it wants.

And so, again, that is why it is so important that we have on-ramps and off-ramps that are regulated and compliant. And I can say that in the U.S., you know, we have great anti-money laundering regulation that requires cryptocurrency exchanges to know their customers, to track all transactions, to collaborate with law enforcement, and they do. But overseas there are exchanges that do not comply with the Fed's regulation. And I think if you ask law enforcement they will tell you that is the biggest challenge for them, vis-a-vis sanctions violators and other criminals.

Senator MENENDEZ. They do not have to convert it into cash. They can use it for payment of necessary goods, and that is equally of value to them.

Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Menendez. Senator Warner is recognized for 5 minutes.

Senator WARNER. Thank you, Mr. Chairman. I appreciate the fact that you and the Ranking Member are holding this hearing. Senator Menendez has talked about how a lot of these issues bleed into the Foreign Relations Committee. I can tell you from the intel

standpoint we have had a number of hearings and discussions on this subject. I think it is how we approach this on a macrobasis, I am not 100 percent sure.

And I can assure you on the ransomware piece there is an awful lot of this being paid out and crypto being used as the payment methodology of choice. And I think if Americans knew how much was paid out on a daily, weekly basis, particularly in Bitcoin, people would be astonished.

I want to take my direction of questions a little bit differently, because crypto writ large comes out of the whole fintech world. We know the fintech world has been basically unregulated. But Mr. Chairman, I am seeing, particularly China—China, Singapore, and indeed Bermuda is ahead of us in terms of using blockchain to create a central bank digital currency. My fear is that in many ways China, which is much further ahead of us on mobile payment systems, on AliPay, and WeChat pay, that these mobile payment systems, which are becoming prevalent, especially in Europe, that they then use as the default, if you have got a mobile payment, the digital yuan.

And we could wake up not dissimilar to where we woke up in 5G, where suddenly when we get alerted to this problem there is already kind of a global answer in place, and we have been a little bit asleep at the switch. Our central bank has been moving slower on this, but this is a very, very aggressive area that China is moving on, and again, using the mobile payment systems as the kind of camel's nose under the tent.

So I would like to hear from the whole panel, starting maybe with you, Professor Walch. How do we think about, and is there an appropriate form to set some international standards, not only on digital currencies but just across this whole field, because my fear is, as your colleague pointed out, we have got fairly decent anti-money laundering laws because, again, of the work of this Committee last year. A lot of the foreign entities do not. But let's stick with, you know, cryptocurrencies writ large and digital currencies backed by central banks as a start-off point. I would love to have the whole panel respond.

Ms. WALCH. Great. So I agree with you that as these cryptosystems are inherently global and international that if there is sort of some regulation surrounding them it will be difficult if it is just one country taking the lead on that, if it is just the U.S. then you risk everyone leaving the U.S. and doing things in other countries that do not have such strict regulatory systems.

I think with a framework of something like FATF, that sets standards for anti-money laundering, that it expects countries to adopt, you could imagine some sort of similar global organization that deals with cryptocurrencies, and come to a consensus about at least what are some of the core things——

Senator WARNER. But as you said, you could imagine. It is not like there is anything out there real time.

Ms. WALCH. Not that I am aware of that is ongoing. I mean, certainly global bodies like the G20 are always discussing this. The Bank for International Settlements facilities discussion of this. But I think it would be helpful if there were, you know, more formal agreements about it.

Senator WARNER. Do your colleagues have any comments, other members of the panel?

Mr. BRITO. Sure. So I will just say two things. You know, we are focused cryptocurrency so we only tangentially look at central bank digital currency. But what I will say is two things. One, I would recommend that you look at an article by Henry Paulson in Foreign Affairs, I think it was earlier this year or maybe last year, where he addressed the question of a Chinese central bank digital currency. And his point, which I took to be persuasive, is that ultimately while they maybe digitizing the yuan, the currency is ultimately the yuan. And this not an attractive currency that people want to hold. And so maybe, you know, it is not really something that threatens the supremacy of the dollar.

The second thing I would say is, so then why is China doing this? I think the main reason that they are doing this is that they do not want to lose control over their own monetary sovereignty. I think their concern is that they are going to get dollarized, not that they are trying to yuan-ize us. They have strict capital controls, as you know, and I think they also want to have strict surveillance of what their population is doing.

In western China, for example, if you stop purchasing alcohol and tobacco, the police will come and check up on you. And they do this because they are looking at your transactions.

Senator WARNER. Final point.

Ms. BELCHER. I would echo that I think it is important that a digital dollar implements measures to protect privacy. I am looking at China and the concerns that have been raised around CBDCs and surveillance.

Senator WARNER. I will just tell you, Mr. Chairman, I think CBDCs, it is coming. If China ends up with the default mobile payment system being kind of the underlying payments for most mobile payments, and it is already happening in Europe and it is increasingly happening in Africa, and then the default currency becomes the digital yuan, I think the panel is dramatically underestimating the potential threat that poses in terms of China's overall plan of technology dominance and the potential. And I, frankly, disagree with former Secretary Paulson on the intent that China brings to this. And I hope, again, that we can spend more time on it, and I appreciate both you and the Ranking Member having this hearing.

Chairman BROWN. Thank you, Senator Warner. Senator Daines from Montana is recognized for 5 minutes.

Senator DAINES. Thank you, Mr. Chairman, and thanks again to all the witnesses for being here today. I truly believe we—we, being the United States—should look to support innovation and be very careful that we do not ever regulate it out of existence. A light touch, I think, is what is called in this situation.

RightNow Technologies, a company that I worked for after I left Procter & Gamble—I was there for 12 years, so we were a pioneer in cloud computing. In fact, when I joined the company we used to call it "hosted companies" and "non-hosted companies" or on-premise. We were an open-source, Linux, Apache, MySQL, PHP, kind of run-and-gun startup, and we got a lot of traction and be-

came the cloud. We were selling a CRM solution. Eventually it was acquired by Oracle.

But I have seen what it is to be on the leading edge of something and then turn to something very exciting. People thought we were crazy back then, and now, of course, the cloud is a massive industry.

Filecoin, which is represented here by Ms. Belcher, provides data storage and access on a decentralized file network and seeks to compete with AWS. This is just one of the many promising uses for cryptocurrencies, and the last thing we should do is regulate these innovators into oblivion.

The innovations occurring in this space are creating high-paying jobs in many places, including my home State of Montana, because we found that some of the brightest people want to live in the best places, and they like the ability to ski, backpack, fish, enjoy our national parks, and they are literally right out their back doors, and yet they are involved in some of the leading edge innovation type tech companies in the world. I think that is generally a very positive thing.

Ms. Belcher, in your testimony you describe Filecoin as "Airbnb for file storage." What type of growth are you expecting for Filecoin in the next 5 years?

Mr. BRITO. Well, it has truly been a massive amount of growth just from October, when we launched, to present. I mentioned that the amount of storage we have right now is truly incredible, and we really hope to see that storage continue to grow as we have seen it growing. And we hope to continue to see it storing humanity's most important information and storing extremely important datasets that need to be preserved for posterity.

Senator DAINES. Thank you, Ms. Belcher.

Mr. Brito, do you see any cryptocurrencies as potentially disrupting the SWIFT global payments network, and could they coexist?

Mr. BRITO. So, no, I do not think there is going to be a disruption of any kind imminently, right. So SWIFT is what allows for transfer of dollars, and dollars make up—I mean, an overwhelming amount of the finance in the world. I do think that they can coexist. You can have both, and, quite frankly, cryptocurrencies is not just about moving money. Cryptocurrency has the word "currency" in it because that is what early pioneers of the technology was the word that they used. But really, these are open networks for verifying distributed ledgers.

And what this means is that you are going to have cryptocurrency networks like Filecoin that store files. That has nothing to do with SWIFT. So they can definitely coexist.

Senator DAINES. Thank you. Ms. Belcher, unlike the private sector, Congress is not fast and not real good at innovating. I think our Founding Fathers, by design, ensured that this city could not move real fast and wanted to keep it limited, to ensure that the private sector innovation and freedom would result in really the greatest of this country, which I believe it has.

How could knee-jerk or overregulation hurt innovation in the jobs you are creating?

Mr. BRITO. Well, I think that it is a myth to say that the cryptocurrency space is not regulated, and I think that as it exists today there are many ways of effectively sensibly applying existing regulations in the cryptocurrency space without needing to add any additional laws that potentially apply specifically to cryptocurrency and might regulate them in a different way.

So just as one example, you know, some people raise issues around cryptocurrency, you know, potential fraud in this space, but there are all sorts of different ways that you can have the CFPB or the FTC go after that kind of fraud. And it does not matter whether you are committing that fraud with cryptocurrency or pen and paper or the phone. And that is just to say that I think that existing regulations do a great job of ensuring the space is regulated without overregulating cryptocurrency specifically.

Senator DAINES. One last quick question for Mr. Brito, and I will need a quick answer. I am in the extra inning here. You previously Stated that you do not believe China's development of a digital yuan is a threat to the dollar. Could you briefly explain why you feel that way?

Mr. BRITO. Sure, because ultimately digital yuan is just digitization of the yuan, and the yuan has all the problems that economists can point out. I mean, most recently, when the COVID pandemic hit, we saw a flight to safety. Did money move to the yuan or did it move massively to the dollar? It came to the dollar.

Senator DAINES. Thank you, Mr. Brito. Thanks for the short answer too. I appreciate it.

Chairman BROWN. Thank you, Senator Daines. Senator Tester from Montana is recognized for 5 minutes.

Senator TESTER. Thank you, Mr. Chairman, and I want to echo the comments of previous folks that asked questions. I appreciate you and the Ranking Member having this hearing.

Before I start my questions I just want to say that the words "decency" and "Mike Enzi" go hand in hand. Mike was a fine man who treated everybody with respect, and somebody that obviously is already missed around here but somebody who will be missed by not only us but by the State of Wyoming. Quality people are not easily replaced, and our thoughts are with Diana and the rest of the Enzi people and the people of Wyoming.

I want to start by taking about—some people here have talked about this being a regulated market, or there is regulation within the market. I do not see a lot of regulation in this market, and my question for all three of you—and as briefly as you can because we can burn 4 minutes on this really quickly—as briefly as you can, do you think this should be a regulated market in a way that is similar to our conventional monetary system? Ms. Walch.

Ms. WALCH. So I have gone back and forth on this for many years, and what has finally crystallized for me is that I think that the cryptofinancial system is different enough from the existing financial system that we need to think carefully about tailoring actual rules that might apply for it.

I think that during the last 10 years there has been a lot of time spent debating about how crypto fits into our very complex, existing financial regulatory scheme.

Senator TESTER. OK. Go ahead, Mr. Brito.

Mr. BRITO. So in the United States we do not regulate technologies. We regulate activities.

Senator TESTER. OK.

Mr. BRITO. So to the extent that there are activities that pose a risk, the same way that they do in traditional financial markets, absolutely it should be regulated.

Senator TESTER. OK. Ms. Belcher.

Ms. BELCHER. I think regulations already are being applied in this space. Just as one example, cryptocurrency on-ramps and off-ramps are heavily regulated. They do KYC. They register with FinCEN. They cooperate with law enforcement. There are reports of suspicious activities. So I do think that there are regulations that are being applied to this space, even though they are not cryptospecific.

Senator TESTER. So I will stay with you, Ms. Belcher. So when we have a situation where we have cybercriminals that ask for money on an essential piece of property, like the Colonial Pipeline, that is critical infrastructure for this country, and one of my constituents turns on the TV and sees that the payment was made in cryptocurrency, what should that person be thinking?

Ms. BELCHER. Well, I think that ransomware is not a cryptocurrency problem. I think it is a cybersecurity problem. And I think where we saw it in the Colonial Pipeline——

Senator TESTER. Time out here for a second. OK. So if you have got a ransom that is being required and it is paid for in cryptocurrency, and albeit some of that cryptocurrency, or maybe all of it, was gotten back—I am not sure I have heard the entire story—cryptocurrency cannot wash their hands and say, "Well, this is not really my problem. It is somebody else's problem." No, like it or not, it is a problem, and cryptocurrency is a part of that problem.

Ms. BELCHER. I think many crimes have also been committed with cash, and I think that in terms of crimes committed with cryptocurrency, we were actually able to get the Colonial Pipeline ransom back, because cryptocurrency is actually a public——

Senator TESTER. Do you think that is going to be the way it is in all cases, because this is going to continue. And by the way, on China's standpoint, I will just tell you this. I think that if we think they are getting rid of the miners because they do not like them, if they did not like them they would treat them like they treat the Uyghurs. They are shipping them around the world because they know these guys can raise hell with our financial system. That is my opinion, and they want to be able to be the big player in the financial industry.

But the real question here is that if, in fact, we have got bad actors out there that are utilizing this technology that nobody ever thought—you know, somebody pointed out, I think it was Senator Reed, that we want to make the good better and get rid of the bad. Well, this is bad stuff that is going on.

Ms. BELCHER. The crime is certainly bad, but I would note that, first of all, I would not blame the technology, and I think it is actually a terrible technology to commit crimes because it creates a public ledger, a public record of each transaction. And so law en-

forcement are able to analyze the public chain, and that is why they were able to get back the Colonial Pipeline ransomware.

Senator TESTER. OK. First of all, I did not thank you guys for your testimony. I appreciate it very, very much. I spent much more time with you, Ms. Belcher, than I was going to with Brito and Walch, but hopefully you will be able to come back again. This is an issue we need more information on so that we can make good decisions. Thank you.

Chairman BROWN. Thank you, Senator Tester. Senator Warren from Massachusetts is recognized.

Senator WARREN. Thank you, Mr. Chairman, and thank you and the Ranking Member for holding this hearing.

So the cryptocurrency boosters argue that crypto is the Yellow Brick Road to a faster, cheaper, and safer financial system that works for everyone, not just for the biggest banks. There is no question that our financial system needs change—big, structural change—and we should be willing to consider how these new technologies can help consumers and our economy.

But as the cryptocurrency market grows, it is also our responsibility to carefully examine these claims and promises about crypto's potential. Now one of the advantages cryptoadvocates claim about Bitcoin and other cryptocurrencies is that they are, quote, "decentralized." Our current system is dominated by a handful of big banks that are mostly free to jack up costs for consumers, to restrict access to financial products, and gobble up smaller competitors, until the big guys become too big to fail.

By contrast, advocates claim that cryptocurrencies and blockchain technology that underlies them decentralize power and control, creating the possibility of a more democratic financial system.

So Professor Walch, that sounds pretty good to me. Has your research shown that crypto is decentralized in this way?

Ms. WALCH. So it is true that in cryptocurrencies you do not have one single central party. So I guess technically you could say yes, it is decentralized. It is more than one. But we have to remember that there are absolutely pockets of power within these systems, particularly the core software developers and the large miners, who can absolutely exploit their position of power to affect users of the systems.

Senator WARREN. So they have the capacity here to manipulate the system. You know, that sounds to me like a lousy tradeoff. Instead of leaving our financial system at the whims of giant banks, crypto puts the system at the whims of some shadowy, faceless group of super-coders and miners, which does not sound better to me.

So let me ask about another claimed benefit of crypto, which is that it is safer and more secure than traditional Government-issued money in the bank. Because the blockchain system is supposed to be difficult to hack, impossible to manipulate, and less prone to network failure, we might not need to worry about things like data breaches or a cyberattack that takes down the network.

Professor Walch, are cryptocurrencies as safe and secure as the proponents claim?

Ms. WALCH. So they certainly have characteristics that enable them to be, you know, resistant to hacking, but it is a misnomer to say that anything is absolutely secure. Again, the parties within the system, such as miners, can exploit their positions to reorganize the blockchain, in some circumstances. That has become a big issue and topic of discussion within Ethereum. This leaves out even the fact that there have been countless hacks of exchanges and stuff that are outside the cryptosystems.

Senator WARREN. OK. Thank you. But even if crypto is not an improvement over our current system when it comes to being more democratic or less hackable, there is one other possible benefit, and it is a big one. Cryptoproponents claim that crypto is safe from the kind of financial crisis that blew up the economy back in 2008. After all, the story goes the motivation behind Bitcoin's creation was to avoid exposure to bank collapses and financial contagion in the traditional financial system.

Professor Walch, for that to be true, crypto would have to be insulated from the risks that make our financial system vulnerable to a crisis, and vice versa. Is that the case?

Ms. WALCH. No. I do not believe that is true. Risks in the cryptosector—software bugs, attacks, anything that could go wrong there—can affect the entire cryptosector but can also, through all these links that have been built between the cryptofinancial system and the traditional financial system, those risks can come across those bridges, those links, to affect people in the traditional financial system, who may never have actually touched crypto in their lives.

Senator WARREN. All right. So look. There is no doubt that we need a stronger, safer, and more inclusive financial system. The biggest banks have too much power, present too many risks to financial stability, and have failed to serve Americans' needs.

The giant banks have created huge problems, but I am not convinced that crypto is the solution. In fact, crypto could be even more dangerous for consumers, more dangerous for the environment, and more dangerous for the stability of our financial system. That is why yesterday I sent a letter to Secretary Yellen in her capacity as head of the Financial Stability Oversight Council, to urge her to lead our regulators in developing a comprehensive and coordinated approach to regulating cryptocurrencies.

Look, all the warning signs are flashing—the hype, the volatility, the wild claims that turn out to be false. As the cryptomarket grows, so do the risks to our financial stability and our economy. Regulators need to do their jobs and step in before it is too late.

Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Warren. Senator Van Hollen from Maryland is recognized.

Senator VAN HOLLEN. Thank you, Mr. Chairman and Ranking Member Toomey, and thank all of you for your testimony today.

I have been a long proponent of getting the Federal Reserve to move quickly to implement the FedNow system, which is a real-time payment system that will eventually help millions of consumers avoid many costly overdraft and other fees that have cost them billions and billions of dollars. At the same time, we have

heard that faster instant payments are often argued as one of the benefits of blockchain technology.

And so my question, starting with Professor Walch is, how do you evaluate these relative benefits and risks, and what are the pros and cons of seeing blockchain and crypto as means to provide faster payments, compared to other possibilities?

Ms. WALCH. So I think one thing to keep in mind is that there have been policy decisions made about the speed at which transactions should be settled on our large global settlement systems, and to my understanding it not technology issues that are controlling the speed. It is policy decisions about what is appropriate and what best manages the risks involved.

As far as settlement issues on cryptocurrencies, they can be fast, but typically because they are probabilistically settled, meaning you do not know for sure that the transaction is final because someone could theoretically come and reorganize the blockchain, they are very different. There is no moment of legal finality on a blockchain. It is you are probably never going to get your transaction changed.

Senator VAN HOLLEN. Mr. Brito, could you just comment on that?

Mr. BRITO. Sure. So I do not think that cryptocurrencies are necessarily competing with what FedNow is trying to do. They are sort of different things. I would say, to what Professor Walch just said, that they are fast, it is probabilistic, but we are building second-layer networks on top of networks like Bitcoin that provide faster and more easily settled transactions, something like the Lightning Network.

And one of the things that these networks allow you to do, that FedNow, I do not think, can allow you to do, is to engage in micro-transactions. So imagine being able to make payments that are pennies, or sub-penny amounts. That is something that is not really economical using our existing financial infrastructure. And so once you can do that, that opens up a whole range of possibilities, of innovations, that can take advantage of that, that we cannot even imagine.

One thing that comes to mind is today the business model of the Web is either advertising—which means tracking—or it is payment, but you cannot just pay for the one article or the one song that you are listening to. You have to pay for a subscription. And so maybe you do not want that.

Imagine a third option that can compete with the ad networks and the big, gated content providers, that allows people to pay per article, per second of streaming video. That is completely new. Imagine going to an airport and instead of paying $20 for a day pass to WiFi you can just pay for the 5 minutes that you need, or the few kilobytes that you need. And at the same time, maybe you share the WiFi in your home and you receive payments from people walking by the street, and you can then use that crypto at the airport.

Senator VAN HOLLEN. Got it. I appreciate that. I do want to follow up, in my remaining time, with some of the issues Senator Warren raised, because Professor Walch, you have written about how software developers and cryptocurrency miners should be seen as fiduciaries. And you talked this morning about how those

were—they are not centralized but they are key choke points in the system and can be manipulated to harm consumers.

Could you talk about a specific example of how a cryptocurrency miner might be able to take advantage of cryptocurrency platform?

Ms. WALCH. Sure. So in many of these proof-of-work systems, like Bitcoin and Ethereum, there are large mining pools, and that means that the other computers who are involved in contributing their power to verify the transactions on the network, you know, entrust that mining pool operator with the power to pick the transactions that are going to go on the ledger and the order in which they will appear. The role and ability to choose the transactions and add a new series of them to the list, to the ledger, rotates around the different miners.

So people say it is disintermediated, but during the moment when the miner is choosing the transactions for a particular block, technologists characterize this as being in "God mode." Right? So those miners can sell, you know, price out how valuable it is to people to front-run transactions, to choose to put one transaction before or behind another. They can do that for their own benefit. And there are huge amounts—we need to get the research before Congress—there are huge amounts of value that miners are exploiting in this way right now, and it is seen as a critical, critical issue to the success of cryptocurrencies and any claims that it has to be immutable, secure, or to lack intermediaries.

Senator VAN HOLLEN. Thank you. And if the other witnesses want to provide, for the record, their opinion on this issue, I do think it is an important consumer protection question.

Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Van Hollen. Senator Smith of Minnesota is recognized.

Senator SMITH. Thank you, Mr. Chair and Ranking Member Toomey. I appreciate this hearing.

Professor Walch, in your prepared testimony you briefly described decentralized finance, or DeFi, and you said that DeFi is a set of financial products mirroring those in the traditional finance system that are rapidly being created.

So over the last 100 years, Congress has enacted this regulatory framework for banking, securities, derivatives, and other key parts of our financial system, and those laws exist for a good reason, right? They are there to protect consumers and the integrity of our financial systems. And we wrote these laws—Congress wrote these laws—based on lessons learned, from stock offerings rife with insider trading and fraud in the 1930s, the boiler room schemes of the 1980s, the risky swaps and derivatives that blew up our economy in 2008.

So it concerns me when I hear about a seemingly unregulated DeFi derivatives market springing up to operate side-by-side with this regulated derivatives market. Last month, CFTC Commissioner Dan Berkovitz said in a speech, and I am quoting here, "Not only do I think that unlicensed DeFi market for derivative instruments are a bad idea, I also don't see how they are legal under the Commodities Exchange Act."

So Professor Walch, do you agree that many of these DeFi instruments are probably operating in violation of the Commodities Exchange Act, or how do you see this?

Ms. WALCH. So I have not analyzed that question particularly, but I see this as we need to look carefully within these systems and see where the same activities are happening and whether there are the same risks. And one of the claims that is made within, you know, cryptosystems is that a lot of these practices are fully automated by software, so, therefore, there is not any particular person to be accountable.

I think we need to press harder on those claims, because there are people who are, you know, running the software who have the keys to make changes to the software. There have been many bugs in these systems that have required the parties who released the software to run these financial transactions, there have been bugs discovered and they had to use their keys that they had failed to disclose that they had, to fix the problem.

So we need to look for where power exists, decide how that power compares to power in our existing financial system, and think about ways to address it.

Senator SMITH. Thank you for that. It seems to me that that could be an argument for going down a path where there is virtually no accountability, if you argue that, you know, there is not a person here. It is just this nameless, you know, technology. Yet you still have what I am so concerned about, which is this unregulated derivatives market operating side-by-side with a regulated derivatives market, and how that could reward rule-breakers and then undermine the system of exchanges and dealers and clearinghouses that Congress has established through a century of experience. Right?

Ms. WALCH. Yeah. I think you need to look for the humans in the system, find them, and ask what they are doing, and whether, you know, you think it poses a risk to other people.

Senator SMITH. Thank you.

I want to touch on a different topic, just in the few minutes that I have left. According to a recent estimate, Bitcoin mining produces about 37 megatons of carbon dioxide each year. So that the same amount of emissions as the entire country of New Zealand. So if you take that on a per-transaction basis, it is estimated that Bitcoin takes 500,000 times more energy to verify a payment compared with a Visa transaction. So that is a lot of energy, especially at a moment where we are, I think, a crucial moment for addressing the need to take action on climate.

If Bitcoin were just this little fad then maybe we could ignore this energy inefficiency. But now Bitcoin is estimated to consume 0.5 percent of all global electricity. Cryptocurrency is increasingly a real concern also as a driver of global emissions, and this clearly is not sustainable.

So I just have a couple of minutes. Would any members of our panel like to comment on this, and what needs to happen to keep cryptocurrencies from becoming such a significant contribute to climate change?

Ms. BELCHER. Thank you for that question, Senator. I would note that different cryptocurrencies have different proof systems that

use different amounts of energy. And when we built the first computer, it was the size of an entire room, but over time technology gets more scalable and sustainable.

And we have also seen major cryptocurrencies switch over to less energy-intensive proof systems, such as Ethereum's recent move to proof-of-stake. And the energy here is being used to achieve particular societal benefits. So for Filecoin, those benefits are creating a decentralized storage network. That is one example.

Senator SMITH. Thank you. I am out of time, but this strikes me as a significant issue. I will follow up, Mr. Brito, since I am out of time. But I think this is a really important issue that we cannot just say we will ride that cost curve down, when we do not have time to do that. Thank you.

Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Smith. Senator Toomey has one more comment or question.

Senator TOOMEY. Thanks very much, Mr. Chairman, and I will ask one question of Mr. Brito. I think Ms. Walch has at least once, maybe a couple of times, alluded to the power of miners, and specifically the power of miners to decide which transactions get put into the block and when. And I think it is fair to say that the insinuation is that they may have motives and self-interest that might cause them to make decisions that would not necessarily be expected by the users, that they are—"nefarious" maybe too strong a word, but that there is a self-interest that might cause them to engage in some kind of distortion.

So how should we think about the miners and their power to decide which transactions get put into the block, and their whole role in the validation process?

Mr. BRITO. Sure. What we have to understand is that miners cannot redirect, steal, or initiate a user's payments. They can, however, affect the order that payments are confirmed on the blockchain during the periodic moments when they successfully mine the next block. So they cannot block you from making a transaction that you want to make. They can just say in what order in the block are you located.

Now this is not a problem in the general case of a person sending money to another person on the Bitcoin blockchain, for example. It has no effect whatsoever. It can be a problem in decentralized exchange transactions, on something like Ethereum, when miners use their ability to order transactions to their advantage.

The same problem exists in traditional financial markets. That is why high-speed traders build proprietary infrastructure to get their trades in as soon as possible. It is why this Committee rightly discusses payment for order flow.

So the problem is very similar. One advantage of decentralized finance is that the blockchain reveals these strategies publicly, rather than happening secretly, thanks to murky internal policies at a large financial institution. Speaking generally, to the extent that we believe that there is a lack of fairness in these trading systems, one of the best solutions is to implement alternative market mechanisms that reduce the advantages of transaction ordering. You can change the design of the exchange. And since the exchange designers do not want this to happen, do not want the miners to

be doing this, the participants certainly do not want this. There is every incentive to change that exchange mechanism, right? Many economists now favor using frequent batch auctions rather than continuous order books for transactions, in order to prevent these problems.

And what is interesting is that if we were going to change from the continuous order book to frequent batch auctions at CME or the New York Stock Exchange, that would require one massive institutional change. With crypto, it is trivially easy for anybody to build a competing exchange that users will go to, and indeed we have seen this, and we are beginning to see this. And also, the developers of the Ethereum network itself do not want to see this, and they are going to be addressing the problem as well.

Senator TOOMEY. Thank you very much. Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Toomey. Thank you all. As Senator Toomey and I were talking, this is one of the most illuminating hearings we have had, and I appreciate you all were persuasive, each in your own way, and thank you for that.

For Senators who wish to submit questions for the record, those questions are due 1 week from today, Tuesday, August 3. To the witnesses, each of you have 45 days to respond to any questions.

Thank you again. The hearing is adjourned.

[Whereupon, at 11:37 a.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF CHAIRMAN SHERROD BROWN

First, I'd like to take a moment to acknowledge the passing of our friend and former colleague, Senator Mike Enzi.

Some of us served with him on this Committee, which he joined in 1997. We remember his kindness, his personal birthday notes that we all looked forward to. He spoke at the Ohio College Presidents Conference we host each year—we always try to bring in leaders of both parties—sharing his insights with Ohio's higher education leaders.

He talked often of bipartisanship—and he meant it.

On a personal note, I think of our long discussions about Boy Scouts. We were both Eagle Scouts, and we often talked about his work to strengthen the Scouting movement.

Our thoughts are with his wife Diana, his children Amy, Emily, and Brad, and with the people of Wyoming.

Since Bitcoin came online in 2009, thousands of these so-called "digital assets"—virtual currencies, cryptocurrencies, stablecoins, investment tokens—have poured into the markets.

All of these currencies have one thing in common—they're not real dollars, they're not backed by the full faith and credit of the United States.

And that means they all put Americans' hard-earned money at risk.

From tech giants like Facebook's Libra—or Diem, or however their PR consultants attempt to rebrand it next—to fly-by-night operations, we've seen far more empty promises than we've seen viable cryptocurrencies.

A cottage industry of decentralized financial schemes has also cropped up alongside these alternative financial products, in the hopes of creating a parallel financial system with no rules, no oversight, and no limits.

They claim to enable "transparency." Their backers talk about the "democratization of banking."

There's nothing "democratic" or "transparent" about a shady, diffuse network of online funny money.

After a decade of experience with these technologies, it seems safe to say that the vast majority haven't been good for anyone but their creators.

This technology is almost never used to buy real goods and services. Which is what any currency is supposed to be used for, after all.

Some cryptocurrency supporters see these technologies as a way to take power back from the Wall Street bankers, whose complicated and opaque financial scheming crashed the economy.

When the only other option appears to be Wall Street, maybe it's hard to blame anyone for putting their faith in cryptocurrency.

I hear the same message over and over from Ohioans: people don't trust banks, and they especially don't trust the biggest banks.

They have been burned over and over again by fees, by minimum balances, by waiting periods, by segregated "second chance" accounts.

And of course, they all remember the crash, the bailouts, the lack of accountability.

But as these technologies have developed, most of them seem to mirror—rather than to challenge—the Wall Street model.

In fact, traditional financial institutions are angling to become the biggest players in these markets, and it's a good bet they'll find even more creative ways to use these new technologies to dodge accountability and put our entire economy at risk again.

We should all be concerned.

Thankfully, President Biden has begun to replace Trump-era financial appointees with real financial watchdogs, who take seriously the job of protecting people's hard-earned money. But the financial recovery remains fragile, as coronavirus variants emerge, and there are still regulators to appoint.

Yes, some of these underlying technologies may have useful applications, beyond evasion of banking and securities laws—those are generally applications outside of finance.

One of those technologies we'll hear about today—Filecoin—uses economic incentives to provide digital storage space.

But if we want a solution to Americans' legitimate fears about our banking system, shady start-ups are not the answer.

We need more community banks that are actually in people's neighborhoods and that understand their lives.

We need No-Fee Accounts, backed by the full faith and credit of the United States through the Federal Reserve, that allow everyone to open a bank account and make online purchases.

And we need to show people there will be real accountability—not just a default to the same Wall Street system where bankers get all the profits and working families end up with all the risk.

We need to make sure the American economy remains the safest and most dependable in the world.

The last thing we should be doing is giving another industry a chance at wrecking that reputation—a reputation our entire economy depends on.

The best thing we can do to protect Americans' money is to adopt smart regulations that protect investors and consumers, and separate the innovators from the extortionists.

I look forward to learning more from our witnesses today.

PREPARED STATEMENT OF SENATOR PATRICK J. TOOMEY

Mr. Chairman, thank you.

Today's hearing provides us an opportunity to learn about the current and potential uses of cryptocurrencies. In short, a cryptocurrency connects one person with another through open, public networks—separate from Government control or other intermediaries.

Cryptocurrencies are a growing part of our lives and economy. The first cryptocurrency—Bitcoin—was implemented in 2009. While there are varying definitions of what is considered a cryptocurrency, there are now thousands of them available in many different forms.

According to a recent University of Chicago survey, 13 percent of Americans bought or traded cryptocurrency in the past 12 months. That's more than half of the total percentage of Americans who invested in stocks during the same period.

Like other currencies, cryptocurrencies may be useful as a store of value or a medium of exchange. However, it's important to acknowledge upfront that a significant impediment to cryptocurrencies becoming a widely used store of value or medium of exchange is their price volatility. That problem could potentially be solved by tying a cryptocurrency to other assets, such as a fiat currency like the U.S. dollar. That's what stablecoins are meant to do.

On the other hand, some cryptocurrencies may prove to be useful as a store of value by serving as alternatives to fiat currencies, like the dollar. They may serve as a store of value because, unlike fiat currencies, the Government can't come along and print trillions of a cryptocurrency.

In this way, cryptocurrencies might complement the role that gold has historically played as a store of value and hedge against inflation. For example, we've seen recently in Venezuela how people can use Bitcoin to store value when a Government devalues its currency.

Also, some cryptocurrencies may prove to be useful as a medium of exchange for buying goods and services. With cryptocurrencies, making payments and conducting transactions may become cheaper, easier, and faster for consumers than it is using traditional currencies.

Cryptocurrencies can be exchanged without the need for an intermediary, such as a bank, which could virtually reduce transaction costs and fees for consumers to zero. In addition, since a person does not need a bank account to use cryptocurrencies, they could increase access to financial services for all Americans.

Beyond these often-discussed uses for cryptocurrencies, there are other ways that the distributed ledger technology underlying crypto can be used. A distributed ledger is a database that shares information across various sites and geographies that is accessible by multiple people. This structure ensures that all of these people can access and verify the data, and reduces the risk of any one central actor manipulating the data.

In my view, the use of distributed ledger technology to have nonintermediated transactions verified in a fool proof way is a powerful technological innovation. This innovation already is having an impact on supply chains, financial services, and securing digital identities. And it has significant potential for verifying the ownership of property, like automobiles, homes, or securities.

In the United States, we spend a lot of time and money to verify property ownership. Distributed ledger technology may provide a way to do this faster and at a lower cost. Over time, it's possible that the application of this innovation may become more important than the usefulness of crypto as a currency.

We're already seeing it have a real world impact. As we know, democracy and individual freedom in Hong Kong are under assault from the Chinese Communist Party. That assault has included the forced closure of a prodemocracy newspaper—*Apple Daily*. But the Chinese Government has not been able to erase *Apple Daily*'s important work.

That's because R-weave, a cryptocurrency network that enables permanent data storage, was used to permanently store portions of the paper. This technology makes it impossible for the Chinese Government to destroy *Apple Daily*'s work no matter what it tries to do. That's just one example.

Today we will hear from two expert witnesses about other current and potential uses of cryptocurrencies. Mr. Jerry Brito is Executive Director of Coin Center, a think tank focused on cryptocurrencies and related topics. He will discuss an array of uses for cryptocurrencies and how these technologies could be further developed. Ms. Marta Belcher is Chair of the Filecoin Foundation. She helped to develop and launch a cryptocurrency—Filecoin—that provides data storage access on a decentralized file storage network.

It's important to note that people have raised legitimate issues about cryptocurrencies. These include their use in illicit activity and their possible effects on monetary policy and on our existing financial infrastructure. We need to discuss and understand these issues, and address them if needed. But we shouldn't lose sight of the tremendous potential benefits that distributed ledger technology offers.

We should also be mindful that private innovation has enabled most of these developments. We should not suppress the concepts of individual entrepreneurship and empowerment that have made this innovation possible.

I look forward to hearing from our witnesses today about the ways cryptocurrencies are impacting and can potentially impact our lives. I hope we will listen to them with open minds.

PREPARED STATEMENT OF ANGELA WALCH

PROFESSOR OF LAW, ST. MARY'S UNIVERSITY SCHOOL OF LAW, RESEARCH ASSOCIATE, UCL CENTRE FOR BLOCKCHAIN TECHNOLOGIES

JULY 27, 2021

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 cryptosystems, the problematic use of language in the cryptospace, and the ways misunderstandings about these systems can contribute to systemic risk.[1] Because my research deals with foundational questions at the heart of this new field, it intersects with many of the fields that come together in cryptosystems, 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 cryptofinancial system over the last decade, and the immaturity of academic and public understanding in this area, I am

---

[1] 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).

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 cryptofinancial 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:

1. 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 cryptofinancial system. I have previously received summer research funding from St. Mary's University School of Law, where I teach.

Key Terms and Concepts

The terminology used in the cryptospace has been challenging since Bitcoin's inception.[2] 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 cryptofinancial system, which makes policymakers' 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, cryptotokens, and digital assets into different buckets (laid out by Goldman Sachs in a recent newsletter)[3] is consistent with how I use these terms and how I see others using them in the cryptospace. 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.[4] [Note that I will use the term "cryptosystems" 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

---

[2] 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).

[3] 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*).

[4] See Shermin Voshmgir and Michael Zargham, "Foundations of Cryptoeconomic Systems", available at *https://assets.pubpub.org/sy02t720/31581340240758.pdf*, for an in-depth discussion of this concept. The study of cryptoeconomic systems is considered a new multidisciplinary field of research.

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."[5]

Digital Assets: "An intangible asset created, traded, and stored digitally. Digital assets in the cryptoecosystem include cryptocurrencies and cryptotokens."[6]

These definitions do not attempt to cover all characteristics of cryptocurrencies, cryptoeconomic systems, cryptotokens, 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 cryptosystems include software developers, miners (sometimes called validators or record keepers), and other stakeholders like users, token holders, or big players in the ecosystem like cryptoexchanges.

In my view, the governance of cryptosystems is critical to understand—who has power, how may it be exercised, and what are the limits of power? Since cryptosystems 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 cryptosystems, 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 cryptoecosystem have demonstrated time and again that parties within cryptosystems (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.[7]

It is also important to note that the cryptofinancial system is characterized by experimental governance. New governance techniques, voting mechanics, and forums are being iterated on in all parts of the cryptoecosystem. I do not critique the innovation efforts here, but it is important to consider the consequences of real-time experimentation on the governance of multibillion-dollar systems with increasing linkages to the traditional financial system.

Functions and Practical Uses of Digital Assets

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

At a high level, digital assets and the cryptofinancial 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 U.S. dollars or other assets in one's wealth portfolio;
- as a way of escaping financial surveillance;
- to enable protest against authoritarian Governments;

---

[5] This definition is slightly revised from Goldman Sachs' definition of "cryptotokens."

[6] This is Goldman Sachs' definition of "digital assets."

[7] 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, and 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 participate in economic activities in the cryptoecosystem, such as the purchase of NFTs (nonfungible 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.[8] 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 cryptospace 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.

Integration With Traditional Financial System

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).[9]

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 cryptosystems, 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 cryptosystems 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.[10] 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.[11]
- Traditional financial institutions offer cryptocustody services.[12]
- Growing use of stablecoins like Tether and USDC from Circle.
- Major investments by venture capital firms into crypto and the cryptoecosystem.[13]

---

[8] 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).*

[9] 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.

[10] 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*).

[11] 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 U.S. currently invest in digital assets).

[12] E.g., Fidelity, Gemini, Coinbase, and others offer this service.

[13] 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 Cryptofund 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. [14]
- Companies providing cryptoservices (e.g., exchanges, Bitcoin mining) are now publicly traded. [15]
- Bitcoin and Ethereum futures have been trading for several years now.
- Major institutions are offering access to cryptofunds to their clients. [16]

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 cryptoevents 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 [17] and the rapid influx of bitcoin miners to places like Texas following China's crackdown on bitcoin mining earlier this year. [18]

Social Impact and Risks

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

Benefits

Proponents argue that cryptosystems 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. [19] 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.

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. [20]

Cryptoproponents use terms like "censorship resistant" and "permissionless" to describe the benefits of cryptosystems, 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 cryptoproponents 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 cryptosystems is inaccurate, and how those inaccuracies serve as sites of hidden risk.

Cryptoproponents 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 cryptosystems are generally unregulated at

---

[14] 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*).

[15] For example, Coinbase, a U.S.-based cryptoexchange went public in April 2021, and several Bitcoin mining companies are publicly traded (e.g., Marathon Digital and Riot Blockchain).

[16] Emily Mason, "About-Face: JPMorgan Opens Crypto Trading to All Clients", *Forbes*, July 22, 2021.

[17] Nelson Renteria, Tom Wilson, and Karin Strohecker, "In a World First, El Salvador Makes Bitcoin Legal Tender", Reuters, June 9, 2021.

[18] 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", *Washington Post*, July 8, 2021.

[19] See Jerry Brito, "The Cash for Electronic Cash", *Coin Center Report*, Feb. 2019 (*https://www.coincenter.org/the-case-for-electronic-cash/*).

[20] 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/*).

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 cryptofinancial 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 cryptotokens 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 financial system, can be sites of risk. It is critical to recognize cryptosystems 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 cryptosystems 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.[21] 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.[22] I note that this theory has been subject to much debate.[23]

Miners or validators are also part of the governance of cryptosystems, 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 cryptosystems as lacking intermediaries and enabling the direct transfer of value between transacting parties, that is technically untrue.[24] Transactions do not appear on the blockchain record unless a miner chooses to put

---

[21] 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).

[22] 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, and Stefan Eich), *Oxford University Press*, 2019.

[23] See, e.g., Raina Haque, et al., "Blockchain Development and Fiduciary Duty", *Stanford Journal of Blockchain Law and Policy* (2019).

[24] See 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 and Aaron Wright, "Blockchain & The Law" (2018), 180 (describing miners or other transaction processors as intermediaries supporting blockchain-based networks).

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 "disintermediation" narrative.[24] 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 cryptospace.

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 cryptotokens 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 cryptosystem, 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 cryptosystems pose risks to society, but my discussion is limited to those I have focused on in my own research.

Realism vs. Idealism

I will close by emphasizing that cryptosystems 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 cryptosystems are simply wrong, and making decisions based on idealized versions of cryptosystems 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 cryptosystem 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.

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.

---

[25] 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*

PREPARED STATEMENT OF JERRY BRITO

EXECUTIVE DIRECTOR, COIN CENTER[1]

JULY 27, 2021

Cryptocurrencies receive much attention these days, but even so, the real use cases of these new technologies are often glossed over. Much cryptocurrency discussion unfortunately leaves the reader with too much breathless hype or knee-jerk condemnation and not enough measured analysis. It is not surprising, then, that some people may walk away with the impression that cryptocurrency is little more than a new iteration of the dot com bubble, without any real value add. Some will say, "There is nothing that can be done with cryptocurrency that cannot be done with sovereign currency that is meritorious and helpful to society." [2]

This is unfortunate, because cryptocurrency technologies have a wide range of use cases that extend far beyond the cloistered circles of Silicon Valley and Wall Street. What's more, cryptocurrencies' technological innovations allow a much broader range of unique applications that traditional sovereign currencies could never provide.

At its core, a cryptocurrency allows any individual to transfer value directly to a recipient anywhere in the world, without needing to rely on a trusted third party in the middle to facilitate the exchange. [3] This seemingly simple function introduces possibilities for a great variety of solutions and improvements in areas of payments, law, security, business processes, and much more.

Here are just a few of the meritorious cryptocurrency applications that will be quite helpful to society—that is, if we allow them to grow.

Direct Digital Payment

Let's start with the simplest use case. We may take it for granted that we can make payments online, but this state of affairs is neither evenly distributed nor always guaranteed. For one, not everyone in the world has access to a bank account or credit card with which they can engage in online commerce. Furthermore, the current system, which relies on third parties to facilitate exchange, is only as good as the trust that we can place in them. Such providers could conceivably go offline due to technical or cybersecurity difficulties, [4] or Governments could push them to prevent certain transactions, [5] or they could mismanage [6] or improperly direct user funds. [7] Whatever the hypothetical, the point is that customers must place considerable trust in the third party to be a responsible and faithful steward of those funds, assuming that individuals have access to those services in the first place.

Cryptocurrencies remove the need to rely on any single trusted third party to make a transaction. In effect, a cryptocurrency replaces a third party like Bank of America or PayPal with the network itself, which is managed by a distributed web of computers all across the world. This means that Alice can make a payment online directly to Bob whenever and wherever she wants, without needing to introduce an-

---

[1] Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using open blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy. This testimony is based on: Andrea O'Sullivan, "Cryptocurrency: What Is It Good For? (A Lot, Actually)", Coin Center, July 30, 2018, *https://www.coincenter.org/cryptocurrency-what-is-it-good-for-a-lot-actually/*; and Jerry Brito and Peter Van Valkenburgh, "The Ideal Regulatory Environment for Bitcoin", Coin Center, August 25, 2020, *https://www.coincenter.org/the-ideal-regulatory-environment-for-bitcoin/*.

[2] Quotation from Rep. Brad Sherman, U.S. House Financial Services Committee, Subcommittee on Capital Markets, Securities, and Investment, "Cryptocurrency Markets", Hearing, March 14, 2018, clip available at: *https://twitter.com/coincenter/status/976182050616152064.*

[3] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", White Paper, October 31, 2008, *https://bitcoin.org/bitcoin.pdf.*

[4] Nicole Perlroth, "Attacks on 6 Banks Frustrate Customers", *New York Times*, September 30, 2012, *https://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html.*

[5] Victoria Guida, "Justice Department To End Obama-Era 'Operation Choke Point'", *Politico*, August 17, 2017, *https://www.politico.com/story/2017/08/17/trump-reverses-obama-operation-chokepoint-241767.*

[6] Kurtis Ming, "Safe Boxes May Not Be Safe After All", CBS Sacramento, July 26, 2018, *https://sacramento.cbslocal.com/2018/07/26/safe-boxes-stolen-drilled/*.

[7] Anna Tims, "Redundancy Payout Nightmare After Bank Transfer Error Sends Stranger Money", *The Guardian*, September 25, 2017, *https://www.theguardian.com/money/2017/sep/25/worker-loses-home-car-bank-money-transfer-error.*

other party that may be cumbersome or costly. This also means that people without access to banking services globally can now take part in digital commerce.

In the U.S. we take it for granted that we can send each other funds effortlessly with our smartphones, but this is not the case everywhere in the world—especially where authoritarian Governments block payments to and from reformers. Just last year, prodemocracy activists in Belarus and anti- police-violence protesters in Nigeria successfully turned to the Bitcoin network to accept donations because local banks would not bank them. [8]

This kind of direct digital exchange is not possible with traditional sovereign currencies. To make a direct exchange with sovereign currencies, individuals will need to meet in person to transact, which can be inconvenient or dangerous. To make a digital payment, they will need to rely on a trusted third party, which can be expensive or unavailable. There is no way to combine direct exchange and digital exchange using a traditional sovereign currency, which is why cryptocurrencies are so unique and value-generating.

Secure Store of Value

Cryptocurrencies are useful beyond their application as a medium of exchange. By eliminating the need to rely on a third party for the issuance and transfer of value, cryptocurrencies empower users to take control of their finances. Transfers can only be made when a user cryptographically approves a specific transaction—an action known as "signing with a private key." This means that the user who holds the private key, and only that user, can control where and when their money is spent.

This use case is crucial in environments where citizens cannot trust that institutions will be responsible stewards of their hard-earned money. Consider the tragic case of a country like Venezuela, where individuals' property and savings can be confiscated by authorities through law or inflation. [9] Many Venezuelans are unfortunately unable to access traditional forms of exit such as emigration or stealthily accruing more stable sovereign currencies. With cryptocurrency, more Venezuelans have an alternative: They can opt to purchase or mine a secure store of value that cannot be confiscated or inflated away by their Government because they alone control their private keys. [10] Indeed, cryptocurrencies are especially popular in Venezuela for precisely this reason. [11]

There is a use for this property for people living in more responsibly managed monetary systems as well. As cybersecurity incidents continue to affect more and greater financial institutions, more people will find their personal information vulnerable to hostile actors. [12] After all, in order to engage with the traditional system of personal finance, we must give over considerable information to banks which are then tied to our credit and debit card numbers. Cryptocurrencies require no such personal information in order to engage in online commerce, and users do not need to trust that financial institutions and their vendors will be able to thwart all of the many daily attacks on their systems.

Microtransactions and Metering

Removing the middleman can also do more than just remove a threat point; it can also reduce the cost to send a transaction. By allowing people to send value directly to another person, cryptocurrencies may prove to be an affordable alternative to other forms of transfer. This means that transactions that may have not made eco-

---

[8] Anna Baydakova, "Belarus Nonprofit Helps Protestors With Bitcoin Grants", CoinDesk, September 9, 2020, *https://www.coindesk.com/belarus-dissidents-bitcoin*; Yomi Kazeem, "How Bitcoin Powered the Largest Nigerian Protests in a Generation", *Quartz Africa*, October 26, 2020, *https://qz.com/africa/1922466/how-bitcoin-powered-nigerias-endsars-protests/*.

[9] Nick Miroff, "How To Fight Hyperinflation in Venezuela? By Seizing Massive Amounts of Cash", *Washington Post*, December 13, 2016, *https://www.washingtonpost.com/news/worldviews/wp/2016/12/13/how-to-fight-hyperinflation-in-venezuela-by-seizing-massive-amounts-of-cash/*; Matt O'Brien, "Venezuela Could Have One Million Percent Inflation. How Is That Even Possible?" *Washington Post*, July 26, 2018, *https://www.washingtonpost.com/business/2018/07/26/good-news-is-venezuela-wont-have-million-percent-inflation-soon-bad-news-is-it-might-later/*.

[10] Rene Chun, "Big in Venezuela: Bitcoin Mining", *The Atlantic*, September 2017, *https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177/*.

[11] John Detrixhe, "Bitcoin Trading in Venezuela Is Skyrocketing Amid 14,000% Inflation", *Quartz*, June 8, 2018, *https://qz.com/1300832/bitcoin-trading-in-venezuela-is-skyrocketing-amid-14000-inflation/*.

[12] Major hacks on entities such as Equifax, Anthem, Marriott, and the Office of Personnel Management are only a few of the high-profile data breaches that have exposed millions of Americans to outside parties. Hacked datasets can be combined to provide an even fuller picture of individual information. See: Garrett M. Graff, "China's Hacking Spree Will Have a Decades-Long Fallout", *WIRED*, February 11, 2020, *https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/*.

nomic sense due to the fees imposed by third parties in the past may now be feasible, which unlocks a range of possibilities.

One of these is microtransactions, which is just what it sounds like: the ability to make tiny transfers of only a few cents (and perhaps fractions of a cent) at a time.[13] When you walk by a gumball machine and decide you want a little treat, it takes very little effort to just whip out a quarter and receive your desired confection. But when you want to purchase the digital equivalent of a gumball online-say, a single music video, or WiFi coverage to check an email for a few minutes, or an in-game upgrade-things quickly become not worth the hassle. You would likely have to create an account with the service in question and would need to have access to some kind of credit card and link it to the service. And because the fees to actually undertake a 25 cent transaction will be greater than the transaction itself, you won't have the option to buy just one item, say, but instead have to pony up for a month's worth of access. This kind of arrangement is obviously just not worth it, so there are a lot of transactions that aren't happening because the existing payments system can't facilitate them.[14]

Cryptocurrencies can, for the first time, make microtransactions for many services economically feasible.[15] Let's say that someone wants to view a paywalled article online, but does not want to purchase a full subscription to that outlet. That person could send a microtransaction to the newspaper's cryptocurrency wallet, which would automatically unlock the article to the payer. The reader benefits by only paying for the content they want, and the newspaper benefits because expanded price discrimination can lead to greater overall engagement. Additionally, microtransactions present an alternative to the advertising model of monetizing content on the web and all the attendant privacy-encroaching tracking it brings with it.[16]

Metering is a special kind of microtransaction. Rather than a per unit price, metered microtransactions allow users to purchase access to a service for an unspecified amount of time. WiFi access provides a good example. Right now, if people want to purchase public WiFi access, they have to purchase a set unit of time for a set price, regardless of whether they only need to send a quick email or check on some data for work. This can be costly and obnoxious to the user, but there is no easy way to meter microtransactions using traditional credit and debit cards for the reasons mentioned above. Cryptocurrency provides a solution for low-to-no fee metering to access these kinds of club goods.

Smart Contracts

People who say that cryptocurrency can't do anything that "sovereign currency" can't also do probably don't understand that cryptocurrencies aren't just a kind of money; they are a kind of programmable money. While our examples so far have focused on simple currency storage and transfers between parties, cryptocurrencies also include scripting capabilities that allow for more complex transactions to occur. These kinds of transactions are known as "smart contracts," and they work because all of the elements of the exchange to take place are entirely digitized.[17]

For example, let's say that Alice would like to gift her granddaughter, Erin, with a sum of money upon her 18th birthday. Today, Alice's option is basically to hire a lawyer to create a trust that will hold the funds and disburse them on the appointed date. Being a technologically savvy grandmother, however, Alice knows that she can simply program a smart contract to do the same thing without having to employ an intermediary. Alice creates a cryptocurrency wallet for herself and another for her granddaughter Erin. Alice sends the equivalent of $10,000 to her wallet and programs a smart contract. The contract is set up so that on the day of Erin's birthday—let's say January 3, 2027—the contract will automatically move the funds from Alice's wallet directly to Erin's, where she will have complete control of

---

[13] Steve Glassman, et al., "The Millicent Protocol for Inexpensive Electronic Commerce", Proceedings of the 4th International World Wide Web Conference, December 1995, *https://www.w3.org/Conferences/WWW4/Papers/246/*.

[14] "Electronic Commerce With Microtransactions", *Computer Weekly*, July 22, 1999, *https://www.computerweekly.com/feature/Electronic-commerce-with-microtransactions.*

[15] Coin Center demonstrated this capability for Congress using the bitcoin lightning network and a lightning-enabled candy dispenser that was built by a Swiss developer, David Knezic, out of off the shelf hardware and open source software. Transactions could be made for fees less than 1/250th of a penny. *https://www.coincenter.org/we-demonstrated-the-bitcoin-lightning-network-in-congress/*

[16] Brave Software, "Basic Attention Token (BAT): Blockchain Based Digital Advertising", White Paper, February 10, 2021, *https://basicattentiontoken.org/static-assets/documents/BasicAttentionTokenWhitePaper-4.pdf.*

[17] Nick Szabo, "The Idea of Smart Contracts", 1997, *https://nakamotoinstitute.org/the-idea-of-smart-contracts/*.

those funds. Once Alice sets the transaction in motion, she no longer has access to the funds, just as if she had created a trust.

And that is just the simplest example. Smart contracts can be deployed any time that a set of digital promises can be enforced by a protocol through which the parties to the promises operate. There are a wide range of hypothetical and currently used applications in the fields of finance, [18] law, [19] and identity. [20]

However, smart contracts are not a kind of magic wand. It is crucial that the parties to a smart contract are absolutely certain that their code will function the way that they intend, and will not be susceptible to attack. There have been high-profile smart contract failures, resulting in millions of dollars in losses. [21] With that caveat in mind, it is likely that routine and simple smart contracts-like the illustration with Alice and Erin above-will be ironed out relatively quickly, and more experience will improve the quality and range of smart contracts available.

Extra-Monetary Applications

The examples above show just a few of the ways that cryptocurrency offers a great expanse of currency-based applications that traditional sovereign currencies simply cannot. But one of the really neat things about cryptocurrencies is that they and the open blockchain networks that underpin them have uses that primarily have little to do with "money" at all.

Our previous examples illustrated how blockchain tokens can be directly transferred in different kinds of ways. But those tokens don't necessarily need to only represent a currency. After all, at the end of the day, it's all just zeros and ones on a computer. So a blockchain token can hypothetically represent anything that can be digitized. And because blockchains are censorship resistant, any entry added to a blockchain can be thought of as a persistent, public, and verifiable record online. This tamper-resistant recordkeeping, however, is only present in open networks with a cryptocurrency or scarce token component.

Consider this story from China: In 2018, a pseudonymous blogger reported that a major pharmaceutical company had been manufacturing and selling unsafe vaccines. [22] Although the story went viral on social media, Government censors went about removing any posts about it online. How could the blogger make sure that his posts would not be blotted out? He put it on an open blockchain network; in this case Ethereum. By sending a small transaction worth a few pennies of ether to their wallet, the blogger was able to attach his expose to the metadata of the transaction, thus immortalizing the report's existence on the internet.

This kind of application is especially crucial in situations where the public must know of some kind of high-level corruption. But there are a number of blockchain efforts to record data for commercial and legal applications as well. Some people envision a title registration service that is entirely or mostly-blockchain-based, which would cut down on the need for costly administration and title insurance. [23] Others are working on projects to offer Dropbox-like services, where a blockchain would facilitate storing users' files in a decentralized manner. [24]

Perhaps more relevant to average Americans are the potential applications of cryptocurrency tamper-resistance to enable identity solutions for cybersecurity. The root cause of many data breaches—such as those at Experian, [25] Equifax, [26]

---

[18] Thaddeus Dryja, "Discreet Log Contracts", MIT Digital Currency Initiative, *https://adiabat.github.io/dlc.pdf*.

[19] Max Raskin, "The Law and Legality of Smart Contracts", 1 *Geo. L. Tech. Rev.* 304 (2017): pp. 305–341, *https://dx.doi.org/10.2139/ssrn.2842258*.

[20] Affan Yasin and Lin Liu, "An Online Identity and Smart Contract Management System", 2016 IEEE 40th Annual International Computer Software and Applications Conference (COMPSAC), June 2016, *https://ieeexplore.ieee.org/document/7552202*.

[21] Andrea O'Sullivan, "Bot-Run Company of the Future Gets Hacked", *Reason*, August 16, 2016, *https://reason.com/2016/08/16/dao-gets-hacked/*.

[22] Kristin Houser, "Chinese Citizens Are Using Blockchain To Warn Each Other of Unsafe Vaccines", *The Byte,* July 25, 2018, *https://futurism.com/the-byte/unsafe-vaccines-china-blockchain*.

[23] Avi Spielman, "Blockchain: Digitally Rebuilding the Real Estate Industry", MIT Center for Real Estate, 2016, *https://dspace.mit.edu/handle/1721.1/106753*.

[24] For examples, see: *https://www.storj.io/*, *https://ipfs.io/*, and *https://sia.tech/*.

[25] Brain Krebs, "Experian API Exposed Credit Scores of Most Americans", Krebs on Security, April 28, 2021, *https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans/*.

[26] Alfred Ng, "How the Equifax Hack Happened, and What Still Needs To Be Done", *CNet*, September 7, 2018, *https://www.cnet.com/tech/services-and-software/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/*.

OPM [27]—is the fact that if an attacker can compromise the password of one individual he may gain access to the personal information of millions of others.

Microsoft is a company that is painfully aware of this vulnerability as it provides the identity infrastructure for over 90 percent of Fortune 500 companies. [28] This is why Microsoft spent years helping develop a decentralized identity standard built on top of Bitcoin. It is called the ION network, it was launched in March, is live and operational, and is now a candidate W3C standard. [29]

By replacing usernames and passwords with decentralized identifiers, [30] the ION network will allow individuals to control their own identities rather than trust data brokers that can be compromised at root. This means that an attacker would no longer be able to compromise just one credential in order to gain access to everyone else's, but would instead have to hack each individually—a massive improvement to cybersecurity.

Other benefits of decentralized identifiers include the ability to verify credentials—helping, for example, to combat disinformation. For example, with ION it will be trivially easy to verify that a photo you're looking at was signed as authentic by a photographer credentialed by the Associated Press. [31] Additionally, because you own your own identity and network of relationships to other identities, we will be able to see the emergence of an open, portable social graph that will allow for competition with incumbent social networks.

What About Regulation?

A cursory review of just a handful of the most high-profile applications of cryptocurrency technologies reveals that these innovations can yield benefits that traditional sovereign currencies never could. It is never a bad thing to wait to get involved with a new technology until you feel that you really understand it—especially when that technology can also be a kind of financial investment. The great thing about cryptocurrencies is that they are entirely voluntary: If a person feels uncomfortable using them, they are in no way obligated to get involved.

There are a lot of very good reasons that cryptocurrency enthusiasts spend so much time improving and building out new infrastructure to bring these innovations to more and more people. And while there are certainly illicit uses of cryptocurrency, that is par for the course for new technologies: from automobiles to the internet. The solution to that is not to throw out the baby with the bath water. A policy environment that preserves for tinkerers and innovators the greatest possible space to develop new and better applications of cryptocurrency technologies will ensure that society gets the most value possible.

What Would Such an Environment Look Like?

As it turns out, with the notable exception of tax policy, the prescription for an enlightened policy environment that balances the risks and benefits of cryptocurrency is essentially the regulatory regime at which the United States has arrived after years of policy evolution. The U.S. regime is not perfect, it can improve, but it gives regulators and law enforcement the tools they need to sensibly address risks and criminal behavior. We divide the policy areas into four general categories of regulation: consumer protection, investor protection, financial surveillance, and tax. We'll go through them one at a time.

Consumer Protection

The purpose of consumer protection regulation is to ensure that businesses who take custody of consumer cryptocurrency for any purpose—whether it is for safekeeping, to provide payments or exchange services, or anything else—are sound and law-abiding. This is typically done through licensing. That is, a business cannot legally offer a service to the public that involves taking custody of consumer funds without first acquiring permission (a license) from the State. The State gives a license to any business that meets certain criteria, including passing a background

---

[27] Brendan I. Koerner, "Inside the Cyberattack That Shocked the U.S. Government", *WIRED*, October 23, 2016, *https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/*.

[28] Apron Shah, "Microsoft Azure: The Only Consistent, Comprehensive Hybrid Cloud", Microsoft Azure blog, September 25, 2018, *https://azure.microsoft.com/en-us/blog/microsoft-azure-the-only-consistent-comprehensive-hybrid-cloud/*.

[29] "Decentralized Identifiers (DIDs) v1.0", W3C Candidate Recommendation Draft, July 20, 2020, *https://www.w3.org/TR/did-core/*.

[30] Ibid.

[31] "Tangents From Coin Center: Daniel Buchner", Podcast, October 21, 2020, *https://www.youtube.com/watch?v=VMzJ3AdhDtI*.

check, posting a bond, satisfying minimum capitalization requirements, and offering specific disclosures to customers.[32]

The key to a sensible consumer protection licensing regime is twofold. First, and most important, it should be clear that the licensing requirement is triggered by custody and nothing else. Second, licensing requirements should be reasonable and nonduplicative.

Taking custody of consumer funds is the activity that creates a risk to consumers (for obvious reasons), and it is that risk that licensing aims to ameliorate. Therefore, if a business provides cryptocurrency services to consumers (possibly including payments or exchange services) but does not take custody of consumer funds, it should be excluded from any licensing requirement. Only if a firm has the ability to lose or steal or otherwise risk consumer funds should it be required to be licensed.

In contrast to this, some foreign Governments have made the mistake of requiring a license from any business that engages in cryptocurrency services, even if no risk to consumer funds can be identified. This is pernicious because it places a burden on firms that have innovated in such a way to provide services to consumers without creating the kind of risk that licensing is meant to address in the first place. The way to avoid that is to have any licensing law turn exclusively on whether the business has "control" of consumer cryptocurrency, and the best statutory definition of "control" available is found in the Uniform Law Commission's Regulation of Virtual-Currency Businesses Act (RVCBA):

> "Control" means . . . [the] power to execute unilaterally or prevent indefinitely a virtual-currency transaction[33]

For firms that do take custody (control) of consumer cryptocurrency, licensing criteria should be clear and sensible. First, in contrast to the United States where a business must acquire dozens of licenses in each state in which it does business, an ideal regulation would be national or transnational (e.g., the E-Money License in the European Union) in scope.[34] Second, the level of regulation imposed by the license should be calibrated to the level of custody risk posed to customers by the business. For example, the RVCBA includes a provision that allows firms to operate without a license (simply by registering) until their business activity exceeds $35,000 annually.[35]

Investor Protection

The purpose of investor protection regulation is to ensure that investors do not face information asymmetries that would put them at a disadvantage. This means ensuring accurate financial reporting issuers of equities, as well as ensuring the fairness of markets. Bitcoin and cryptocurrencies like it are not securities, in part because there is not a firm or person who runs the Bitcoin network or issues bitcoins. It is instead more accurately classified as a commodity.[36] Therefore, regulations that apply to securities and securities markets should not apply to Bitcoin and cryptocurrencies like it. In contrast to the United States, which employs a court-made test for determining whether an asset qualifies as an "investment contract," most other countries list in statute what assets are securities. The ideal regulatory policy should simply ensure that Bitcoin and cryptocurrencies are not treated as securities.

As far as market regulation is concerned, an ideal policy would be to simply ensure equal treatment between markets in cryptocurrency and commodities. Typi-

---

[32] See, generally: Marco Santorini, "What Is Money Transmission and Why Does It Matter?" Coin Center, April 7, 2015, *https://www.coincenter.org/education/policy-and-regulation/money-transmission/*; See also, e.g., Coinbase license list, accessed June 28, 2021, *https://www.coinbase.com/legal/licenses.*

[33] "Uniform Regulation of Virtual-Currency Businesses Act", National Conference of Commissioners on Uniform State Laws, drafted at the ULC Annual Conference, San Diego, CA, July 14–20, 2017, *https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=bd2ebf37-48a6-1d1e-8644-a9869bb-4f0e7&forceDialog=0.*

[34] Peter Van Valkenburgh, "The Need for a Federal Alternative to State Money Transmission Licensing", Coin Center, January 2018, *https://www.coincenter.org/the-need-for-a-federal-alternative-to-state-money-transmission-licensing/*.

[35] Supra at 33.

[36] This has been stated policy at both the SEC and the CFTC. See: Neeraj Agrawal, "SEC Chairman Clayton: Bitcoin Is Not a Security", Coin Center, April 27, 2018, *https://www.coincenter.org/sec-chairman-clayton-bitcoin-is-not-a-security/*; William Hinman, "Digital Asset Transactions: When Howey Met Gary (Plastic)", Remarks at the Yahoo Finance All Markets Summit: Crypto, San Francisco, CA, June 14, 2018, *https://www.sec.gov/news/speech/speech-hinman-061418*; "CFTC Statement on Self-Certification of Bitcoin Products by CME, CFE and Cantor Exchange", Commodity Futures Trading Commission, December 1, 2017.

cally, it is not markets for commodities themselves that are regulated, but commodity derivatives markets that are subject to regulation. Alternatively, foreign exchange market regulation could serve as a model for cryptocurrency exchange regulation or new authority could be given to a Federal supervisor, such as that proposed in the Digital Commodity Exchange Act.[37]

Financial Surveillance

The purpose of financial surveillance laws (better known as anti–money-laundering regulation) is to deputize private businesses as criminal investigators for the State.[38] Generally these laws apply only to a defined class of business referred to as "financial institutions."[39] Regulated financial institutions must collect identifying information about their customers, as well as surveil their customer's activities and report detailed information about certain specified transactions (or potentially all transactions) to the financial surveillance regulator, which will in turn share that information with law enforcement and national security agencies.[40] Throughout this process customer information is collected and transmitted to the Government without a search warrant, and, in some cases, without any independent legal process whatsoever.[41] Persons engaged in a variety of cryptocurrency activities may or may not be classified as financial institutions and be obligated to surveil their customers or transactional counterparts.[42]

As far as financial surveillance is concerned, an ideal policy would be to require a warrant for any State collection of personal financial data from a financial institution including businesses facilitating cryptocurrency activities. This, however, would be an extreme shift in policy; banks have been subject to financial surveillance laws in the U.S. since the 1970s, and the Supreme Court found long ago that bank customers have no reasonable expectation of privacy over records that they willingly hand over to banks while transacting.[43] Similar regimes have proliferated across the world thanks to international standards-setting bodies such as the Financial Action Task Force.[44] Short of reviving judicial oversight and a warrant requirement for the mass collection of customer financial data by law enforcement, a pragmatic policy is to seek equal treatment as between cryptocurrency businesses and traditional financial institutions. This means that only those businesses that hold and control customer cryptocurrency (as in our definition from consumer protection above) should be classified as regulated financial institutions. Noncontrolling cryptocurrency businesses such as miners, node-operators, software developers, or minority key-holders in a multi-sig arrangement, should never be classified as financial institutions. Individuals transacting on their own behalf (buying and selling, donating, or paying for goods and services) should also never be classified as financial institutions. Generally speaking, this is the current policy of FinCEN.[45]

Taxation

Ideally, the IRS should state clearly and in detail how cryptocurrency transactions will be taxed as this may not be intuitive given the novelty of cryptocurrencies as assets including how to account for basis in calculating capital gains.[46] There

---

[37] Rep. Michael K. Conaway, "Digital Commodity Exchange Act of 2020", H.R. 8373, House Agriculture Committee, 116th Congress, introduced September 24, 2020, *https://www.congress.gov/bill/116th-congress/house-bill/8373.*

[38] Peter Van Valkenburgh, "Electronic Cash, Decentralized Exchange, and the Constitution", 0Coin Center, March 2019, *https://www.coincenter.org/electronic-cash-decentralized-exchange-and-the-constitution/#iii-electronic-cash-decentralized-exchange-and-the-fourth-amendment (Section III: Electronic Cash, Decentralized Exchange, and the Fourth Amendment).*

[39] 31 U.S.C. §5312.

[40] Id.

[41] Supra n. 38.

[42] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", Financial Crimes Enforcement Network, FIN-2013-G001, March 18, 2013, *https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf*; and "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies", Financial Crimes Enforcement Network, FIN-2019-G001, May 9, 2019, *https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.*

[43] Supra n. 38 and California Bankers Assn. v. Shultz, 416 U.S. 21 (1974).

[44] "About", Financial Action Task Force, accessed July 24, 2021, *https://www.fatf-gafi.org/about/*.

[45] "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies", Financial Crimes Enforcement Network, FIN-2019-G001, May 9, 2019, *https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.*

[46] James Foust, "A Duty To Answer: Six Basic Questions and Recommendations for the IRS on Crypto Taxes", Coin Center, April 2019, *https://www.coincenter.org/a-duty-to-answer-six-basic-questions-and-recommendations-for-the-irs-on-crypto-taxes/*.

should also be a threshold in the amount gained below which no tax is due. Without such a de minimis exemption from capital gains taxation, a cryptocurrency user could trigger a taxable event every time she pays for a good or service rendering cryptocurrencies too complicated for micropayments or other simple payments use.[47]

Cryptocurrency block rewards from mining or staking on cryptocurrency networks should not be taxed as income when they are created. These rewards are best analogized to fruit that has ripened on the taxpayer's land, crops grown in her fields, or precious metals mined from her soil. Applying a tax liability at the moment the new value is created generates extreme accounting difficulties and overtaxes the citizen. Instead, should a country wish to collect taxes related to mining or staking activities, it should tax them when they are sold by the miner or staker.[48]

Conclusion

As the above lays out, there are many use cases for cryptocurrencies that can be beneficial to society. Allowing this technology to flourish can also help maintain the position of the United States as the home to global innovation. In order for us to achieve this promise we must also carefully consider the ideal regulatory environment that both fosters innovation and adequately protects consumers. As noted at the outset, the regulatory regime in the United States goes in the right direction.

Like the early internet, there are real, live uses of cryptocurrency networks today, but we can only see glimpses of the truly world-changing applications to come. The Clinton administration successfully pursued a deliberate policy of avoiding undue restrictions of the internet.[49] To reap the benefits of cryptocurrency networks we should have the wisdom to do the same today.

PREPARED STATEMENT OF MARTA BELCHER

CHAIR, FILECOIN FOUNDATION

JULY 27, 2021

Thank you, Chairman Brown, Ranking Member Toomey, and Committee Members, for inviting me to testify today.

I'm Marta Belcher. I serve as Chair of the Filecoin Foundation, one of many companies working on a cryptocurrency called Filecoin. The question posed by this hearing is, "What Are Cryptocurrencies Good For?" Our answer to that question is that cryptocurrency can be the foundation for a better internet—an alternative to big tech that puts people in control of their own data, protects user privacy and security, and permanently preserves humanity's most important information. Today, I would like to explain how.

Cryptocurrency makes it possible to send monetary value across the globe instantly and securely—just as easily as you can send information over the internet by attaching a file to an email. That is to say, cryptocurrency does for monetary value what the Internet did for information.

For me, the most important thing about cryptocurrency is that it creates the ability to program money. In other words, you can write computer code that automatically transfers value upon a condition being met. For example, you could write a computer program that says, for every second of a song that I play, automatically transfer the equivalent of a millionth of a cent from me to the songwriter. This can happen instantly and automatically, with no intermediary between us, even across borders. This kind of transaction would be untenable using traditional payment systems.

The cryptocurrency technology I work on—Filecoin—uses that same programmable money concept to create a decentralized file storage network. If you have extra storage space on your computer hardware, you can "rent it out" to others who will pay you to store their files (or pieces of their files, so that only the file owner can put the pieces back together). A computer program will regularly check that the

---

[47] There is already a de minimis exemption from capital gains taxation for foriegn currencies and legislation has been introduced to apply a similar sensible standard to cryptocurrencies. See: Mike McSweeney, "New Congressional Bill Seeks De Minimis Tax Exemption for Smaller Crypto Transactions", Office of Congressman David Schweikert, January 16, 2020, *https://schweikert.house.gov/media-center/in-the-news/new-congressional-bill-seeks-de-minimis-tax-exemption-smaller-crypto.*

[48] Mattia Landoni, "Dilution and Its Discontents: Quantifying the Overtaxation of Block Rewards", Coin Center, August 2020, *https://www.coincenter.org/dilution-and-its-discontents-quantifying-the-overtaxation-of-block-rewards/*.

[49] Jerry Brito, "How the SEC and CFTC Can Address Cryptocurrency While Preserving U.S. Innovation", Coin Center, January 25, 2018, *https://www.coincenter.org/how-the-sec-and-cftc-can-address-cryptocurrency-while-preserving-us-innovation/*.

files are still being stored on your computer and, if so, automatically compensate you with cryptocurrency. It's like Airbnb for file storage: storage providers rent out their extra storage space to earn Filecoin, and users spend Filecoin to store their files on other people's computers.

That may sound like a niche use case, but we believe this could be a foundational technology for the next generation of the Internet. Today's Internet is centralized. The vast majority of data making up the many websites Americans use every day sits in data warehouses owned by just three companies: Amazon Web Services, Microsoft Azure, and Google Cloud. We have repeatedly seen these companies suffer blackouts, and vast swaths of the Web go down for hours, including websites that are massive contributors to the American economy. That's the problem with having single points of failure.

We believe you can create a better version of the Web if you combine the storage capacity and computing power on all of our individual devices into a supercomputer-like network, and store multiple copies of data across those devices. On this decentralized version of the Internet, websites will stay up even if some nodes fail, and the availability of information is not dependent on any one server or company. This provides a more robust platform for humanity's most important information.

Filecoin provides the incentive for people to contribute storage to that decentralized Internet. And these incentives work. Since launching last October, nearly 3,000 Filecoin storage providers have contributed nearly 8 exabytes of storage capacity. To put that in perspective, that could store all of the written works of mankind in all languages from the beginning of recorded history to today, 10 times over. And that storage space is being used to preserve humanity's most important information. As just one example, the Starling Lab—a project of Stanford and USC—uses the Filecoin network to permanently preserve the USC Shoah Foundation's archive of 55,000 video testimonies of genocide survivors.

Filecoin is just one use of cryptocurrency, but it demonstrates how being able to program money—to instantly, automatically send microtransactions across the world—can create economic incentives that enable entirely new technologies.

There are already thousands of projects building other cryptocurrency applications, from automatically paying music royalties, to compensating people when their data is used, to paying journalists for each view of an article, to incentivizing consumers to use renewable energy. Many of these projects will fail, but some may move technology forward in ways we cannot yet begin to imagine.

This technology is in its early days, and this stage of development for cryptocurrency is often compared to the Internet of the early '90s. It would have been a mistake, in 1995, to believe that we understood then what the Internet was good for. I would urge the Committee to embrace the possibility that cryptocurrency's uses might be just as expansive, and to ensure that innovation in this space can continue to thrive.

I look forward to your questions. Thank you.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM ANGELA WALCH

Q.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?

A.1. 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 cryptofinancial system.

Actors in the traditional financial system, including commercial banks, are responding to the growth of the cryptofinancial 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 cryptofinancial 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 cryptofinancial 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 cryptosystems. There are no longer sharp divisions between the traditional financial system and the cryptofinancial system.

Q.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?

A.2. 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 U.S., 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 U.S response to crypto, contributing to uncertainty about which regulatory agency should be addressing which cryptorelated 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 U.S. 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 cryptoissue. 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.

Q.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?

A.3. There are a number of difficulties that State and Federal regulators face in these prosecutions. A nonexhaustive list includes those described below.

1. Each cryptosystem 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 cryptosystems 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 cryptosystem is fast-moving and evolving. At this point, there are no fully "ossified" cryptosystems, 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 cryptosystems 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 nonsecurity/commodity categorization for stare decisis reasons.

There remains dispute over which digital assets are securities and which are commodities. The SEC has been criticized by the cryptoindustry 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

---

[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, "Deconstructing '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.

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

Limited staff and funding is also a hindrance to prosecution, particularly given the exploding scale of the cryptofinancial 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 CFT" 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.

Q.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 antitrafficking projects?

A.4. 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 cryptofinancial 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. Cryptoproponents argue that applying the AML framework from the banking world to them does not make sense because cryptotransactions are not intermediated, but direct from person to person, meaning that there is no party within cryptotransactions for AML rules to target. I believe that this is inaccurate, given the middleman role that miners/validators play in every cryptotransaction. 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.

The second issue related to AML and crypto is that cryptoproponents, 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

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

[4] See, e.g., Gary Gensler, Chair of the SEC, Written Testimony before the Senate Committee on Banking, Housing, and 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 5 years later, though, that number had decreased by about 4 percent.").

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.

Q.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?

A.5. 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.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR SINEMA FROM ANGELA WALCH

Q.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 cyberthreats 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?

A.1. 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 cryptosystems and there are various attack vectors that exist.[1] It is important to recognize that parties within cryptosystems, such as the miners/validators and software developers, also pose attack risks to the system, much as "insider" at-

---

[5] See Maggie R. Hu, Adrian D. Lee, and 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).

[1] 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).

tacks pose cybersecurity risks in non-blockchain systems.[2] Though cryptosystems 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.[3] 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.[4]

Further, viewing cryptocurrency transactions as "direct" or "peer to peer" is problematic as they are intermediated by miners and validators within the cryptosystems. 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.

Q.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?

A.2. 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 cryptofinancial 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. Cryptoproponents argue that applying the AML framework from the banking world to them does not make sense because cryptotransactions are not intermediated, but direct from person to

---

[2] See Ivan Homoliak, Flavio Toffalini, Juan Guarnizo, Yuval Elovici, and Martin 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).

[3] See Ax Sharma, "Cryptocurrency Launchpad Hit by $3 Million Supply Chain Attack", *ArsTechnica*, Sept. 17, 2021.

[4] For a discussion of several of these, see 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, and 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);

person, meaning that there is no party within cryptotransactions for AML rules to target. I believe that this is inaccurate, given the middleman role that miners/validators play in every cryptotransaction. 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.

The second issue related to AML and crypto is that cryptoproponents, 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.

Q.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 U.S. CBDC. Would a blockchain-based U.S. 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 U.S. CBDC?

A.3. Global research into CBDCs is looking broadly into many possible technology implementations, including blockchain-based systems.[5] 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.

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 tech-

[5] 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 and Rainer Bohme, "The Technology of Retail Central Bank Digital Currency", *BIS Quarterly Review*, pp. 85–96 (Mar. 2020).

nology 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. [6]

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. [7] Others, like Sweden, are trialing CBDCs using permissioned blockchain systems. [8] 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.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM JERRY BRITO

Q.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?

A.1. I don't believe it necessarily follows that if Americans decide to hold digital tokens in significant amounts that this will mean that commercial banks will face a compression of margins. It would not be the case any more than the fact that Americans holding stocks and bonds affect bank margins. Cryptocurrencies are a new commodity asset class similar to gold or oil. Americans will hold cryptocurrency tokens as an investment or for consumptive use. I do not believe that Americans will use cryptocurrencies as a substitute for dollars as currency. [1]

Q.2. Can you explain more how a person who does not have access to a bank account or does not have access to the internet can obtain cryptotokens and transact in cryptocurrencies?

A.2. Someone without a bank account or internet access can obtain cryptocurrency by trading cash for cryptocurrency. This can be

---

[6] 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).

[7] 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).

[8] 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).

[1] See Andrea O'Sullivan, "How Do Cryptocurrencies Affect Monetary Policy?" Coin Center, June 20, 2018, *https://www.coincenter.org/education/policy-and-regulation/how-do-cryptocurrencies-affect-monetarypolicy/*.

done at an automated teller machine or via an in-person transaction. To possess cryptocurrency one does not need access to a computer; one only needs to be able to hold a series of letters and numbers (call it a password) that controls a certain amount of cryptocurrency units. This can be done on paper,[2] with tamper-proof coins,[3] or even by memorizing the password.[4] That all said, it is very unlikely that any significant number of persons will use these methods. The question posed is akin to asking, how can a person who does not have access to the internet make use of email or online shopping? While one can conceive of ways to do so, such as using internet cafes or libraries, it is likely not something that persons without internet access will pursue. This would be a significant concern if cryptocurrency were to replace the dollar, but as I explained above I do not believe that is a serious possibility. A more likely concern is that physical cash is replaced by a national digital currency, something that would indeed affect those persons who do not have bank accounts or internet access.

Q.3. What opportunities exist for redress in terms of smart contracts whereby an issue in the program's code results in an unintended consequence for both parties involved?

A.3. There are a few ways to address a situation where an undetected bug in a smart contract generates an unexpected result for the parties involved. First, depending on the circumstances, parties may be able to contact and seek redress from counterparties. Second, to the extent the smart contract was marketed as fit for a particular purpose, there may be recourse under common law fraud claims and Unfair and Deceptive Acts and Practices laws at the Federal and State levels.[5]

That all said, smart contracts are typically open source code (i.e., legible by anyone and free of copyright protections) and, if executed, will operate in a deterministic manner, so there is little reason to expect recourse beyond contract or UDAP. As an analogy, imagine one comes across the plans for a wood folding chair on a woodworker's personal website. One downloads the plans and follows them to a tee, yet at the end the chair does not fold properly because the woodworker who drew up the plans made a mistake. What recourse does one have? One doesn't have a contract with the woodworker, nor did the woodworker market his plans or make any representations about them. It's a case of mutual mistake since one didn't spot the error any more than the woodworker did.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR SINEMA FROM JERRY BRITO

Q.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 cyberthreats to institutions in both the public and private sectors

---

[2] "Paper Wallet", Bitcoin wiki, accessed September 16, 2021, *https://en.bitcoin.it/wiki/Paper-wallet*.

[3] "Casascius Physical Coins", Bitcoin wiki, accessed September 16, 2021, *https://en.bitcoin.it/wiki/Casascius-physical-bitcoins.*

[4] "Brainwallet", Bitcoin wiki, accessed September 16, 2021, *https://en.bitcoin.it/wiki/Brainwallet.*

[5] 15 U.S.C. §45, see also *https://www.nclc.org/images/pdf/udap/report-50-states.pdf.*

through the use of alternative methods of file storage, direct transactions, and other use-cases for cryptocurrencies?

A.1. Yes. For example, the root cause of many data breaches—such as those at Experian,[1] Equifax,[2] OPM[3]—is the fact that traditional centralized databases are particularly vulnerable: if an attacker can compromise the password of one individual he may gain access to the personal information of millions of others.

Microsoft is a company that is painfully aware of this vulnerability as it provides the identity infrastructure for over 90 percent of Fortune 500 companies.[4] This is why Microsoft spent years helping develop a decentralized identity standard built on top of Bitcoin. It is called the ION network, it was launched in March, is live and operational, and is now a candidate W3C standard.[5]

By replacing usernames and passwords with decentralized identifiers,[6] the ION network will allow individuals to control their own identities rather than trust data brokers that can be compromised at root. This means that an attacker would no longer be able to compromise just one credential in order to gain access to everyone else's, but would instead have to hack each user individually—a massive improvement to cybersecurity.

Other benefits of decentralized identifiers include the ability to verify credentials—helping, for example, to combat disinformation. To explain, with ION it will be trivially easy to verify that a photo you're looking at was signed as authentic by a photographer credentialed by the Associated Press.[7] Additionally, because a decentralized network allows you to own your own identity and control your network of relationships to other identities, there can be an open, portable social graph capable of competing with incumbent, proprietary social networks.

Similarly, decentralized file storage networks like Filecoin, Sia, and Storj, allow individuals and firms to take advantage of cloud data storage without having to trust the security of a single service provider like Google or Amazon. Instead, user data is chopped into many pieces, those pieces are individually encrypted with a key that only the user controls, and redundantly stored across nodes of the network. This means there is no single point of failure for an attacker to exploit—a vast improvement over today's standard model.

Q.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

---

[1] Brain Krebs, "Experian API Exposed Credit Scores of Most Americans", Krebs on Security, April 28, 2021, *https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans/*.

[2] Alfred Ng, "How the Equifax Hack Happened, and What Still Needs To Be Done", CNet, September 7, 2018, *https://www.cnet.com/tech/services-and-software/equifaxs-hack-one-year-later-a-look-back-at-how-ithappened-and-whats-changed/*.

[3] Brendan I. Koerner, "Inside the Cyberattack That Shocked the U.S. Government", *Wired*, October 23, 2016, *https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/*.

[4] Apron Shah, "Microsoft Azure: The Only Consistent, Comprehensive Hybrid Cloud", Microsoft Azure blog, September 25, 2018, *https://azure.microsoft.com/en-us/blog/microsoft-azure-the-only-consistent-comprehensive-hybrid-cloud/*.

[5] "Decentralized Identifiers (DIDs) v1.0", W3C Candidate Recommendation Draft, July 20, 2020, *https://www.w3.org/TR/did-core/*.

[6] Ibid.

[7] "Tangents From Coin Center: Daniel Buchner", Podcast, October 21, 2020, *https://www.youtube.com/watch?v=VMzJ3AdhDtI*.

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?

A.2. The key to combating illicit use of cryptocurrencies is ensuring proper regulation of the on- and off-ramps from the traditional financial systems. Illicit actors will always ultimately seek to cash out their illicit gains.[8] Exchanges and other off-ramps are the choke points at which they can be identified and funds seized. Law enforcement has had great success disrupting illicit activity using a combination of blockchain analysis and KYC information collected by exchanges. The problem is that not all exchanges comply with anti-money laundering laws, in particular foreign exchanges based in Asia and Eastern Europe. This is the biggest gap in law enforcement's ability to target criminal activity, especially when the States that have such rogue exchanges within their borders do little to assist U.S. investigators. Law enforcement needs greater help addressing these rogue exchanges overseas. To the best of my knowledge, all U.S.-based exchanges comply with BSA requirements and actively cooperate with law enforcement. Increasing regulatory burdens on these exchanges, or even introducing requirements they cannot possibly comply with, will not improve matters and will instead cede further ground to those who disregard the law.

Q.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 U.S. CBDC. Would a blockchain-based U.S. 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 U.S. CBDC?

A.3. The greatest potential benefits from adopting a CBDC are related to the interoperability in payments it could facilitate. This depends, of course, on an open and permissionless design.[9] On the other hand, the greatest threat of a CBDC is to privacy. One can imagine a CBDC design that gives the Government and corporations full visibility into all citizens' transactions—indeed this is how China's CBDC works.[10] Add to this the elimination of cash and the result is an economy in which all transactions are intermediated and thus surveilled. This would be at complete odds with the liberal values of an open society.[11] Luckily, cryptocurrency

---

[8] The idea that one would be able to live and operate entirely within a cryptocurrency economy is fanciful. See Andrea O'Sullivan, "How Do Cryptocurrencies Affect Monetary Policy?" Coin Center, June 20, 2018, *https://www.coincenter.org/education/policy-and-regulation/how-do-cryptocurrencies-affect-monetarypolicy/*.

[9] Peter Van Valkenburgh, "Open Matters: Why Permissionless Blockchains Are Essential to the Future of the Internet", Coin Center, December 2016 (see subsection IV.A.ii. "Why Open Is Critical for Cash").

[10] Raymond Zhong, "China's Cryptocurrency Plan Has a Powerful Partner: Big Brother", *New York Times*, October 18, 2019, *https://www.nytimes.com/2019/10/18/technology/china-cryptocurrency-facebook-libra.html* ("Chinese officials use something of an oxymoron to describe what their new currency will offer: 'controllable anonymity. . . . As long as you aren't committing any crimes and you want to make purchases that you don't want others to know about, we still want to protect this kind of privacy,' Mr. Mu, the deputy director of the central bank's payments department, said in another recent online lecture on China's cryptocurrency plans.").

[11] Jerry Brito, "The Case for Electronic Cash", Coin Center, February 2019, *https://www.coincenter.org/the-case-for-electronic-cash/*.

technology shows us that we have the technical capacity to design a CBDC in such a way that it is open, permissionless, and as private as physical cash. [12]

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM MARTA BELCHER

Q.1. Digital-currency based systems could magnify concerns surrounding illicit activity and consumer risk. What recommendations do you have pertaining to consumer devices to safeguard data and combat fraud and identity theft?

A.1. We can—and already do—sensibly apply existing laws and regulations to the cryptocurrency space to address concerns regarding illicit activity and consumer risk.

It is a misconception that cryptocurrencies are unregulated. The onramps and offramps where people buy, sell, and custody cryptocurrency are heavily regulated. These onramps and offramps are chartered banks, trust companies, or State-licensed money transmitters. As financial institutions under the Bank Secrecy Act, they register with the Financial Crimes Enforcement Network (FinCEN), verify their customers' identities, and share details of suspicious transactions with law enforcement.

In addition, if someone commits fraud, it does not matter what technology they use to do so. If someone commits fraud, actions can be taken by the Consumer Financial Protection Bureau, the Federal Trade Commission, the Commodity Futures Trading Commission, the Securities and Exchange Commission, and State attorneys general, in addition to private causes of action—regardless of whether the fraud is committed using cryptocurrency, cash, the phone, email, pen or paper, or any other technology.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR SINEMA FROM MARTA BELCHER

Q.1. The entertainment industry creates thousands of jobs and provides Arizonans with the opportunity to enjoy art, theatre, and music. Do you believe that the cryptocurrencies have great potential to support artists' income through the use of programmed royalty transactions?

A.1. Yes, cryptocurrencies have the potential to—and already do—support artists' income through programmed royalty transactions.

Cryptocurrency creates the ability to program money—in other words, to write computer code that automatically transfers value upon a condition being met. For example, you could write a computer program that says, for every second of a song that a user plays on a computer, automatically transfer the equivalent of a millionth of a cent from the listener to the songwriter. This can happen instantly and automatically, with no intermediary between the user and the songwriter, even across borders.

There are already many cryptocurrency applications that use this technology for paying music royalties. For example, Audius is a

---

[12] Matthew Green and Peter van Valkenburgh, "Without Privacy, Do We Really Want a Digital Dollar?" Coin Center, April 30, 2020, *https://www.coincenter.org/without-privacy-do-we-really-want-a-digital-dollar/*.

music streaming platform that uses the Interplanetary File System's decentralized technology to directly link artists with their listeners, to enable artists to control and monetize their own music.

Q.2. 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 cyberthreats 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?

A.2. At the Filecoin Foundation, we are using cryptocurrency technology to build a decentralized version of the Web—an alternative to Big Tech that puts people in control of their own data, protects user privacy, and enhances cybersecurity.

Today's Internet is centralized. The vast majority of data making up the many websites Americans use every day sits in data warehouses owned by just three companies: Amazon Web Services, Microsoft Azure, and Google Cloud. We have repeatedly seen these companies suffer blackouts, and vast swaths of the Web go down for hours, including websites that are massive contributors to the American economy. That is the problem with having single points of failure.

The Filecoin Foundation is working to create a better version of the Web by combining the storage capacity and computing power of many individual devices into a supercomputer-like network, and storing multiple copies of data across those devices. On this decentralized version of the Internet, websites will stay up even if some nodes fail, and the availability of information is not dependent on any one server or company. This provides a more robust platform for humanity's most important information.

Q.3. 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?

A.3. It is a misconception that cryptocurrencies facilitate crime. Cryptocurrencies like Bitcoin are not anonymous; they are pseudonymous. Bitcoin's ledger publicly and permanently records all transactions, including the public key (which is similar to a username) of the people making the transactions. This public ledger can help law enforcement trace bad actors. For example, after the recent Colonial Pipeline ransomware attack, law enforcement officials were able to recover the Bitcoin that had been paid in ransom within days of the attack.

Q.4. 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 U.S. CBDC. Would a blockchain-based U.S. 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 U.S. CBDC?

A.4. Central Bank Digital Currencies raise important questions about privacy and surveillance. In order to protect civil liberties, it is critical that CBDCs implement safeguards to ensure that individuals can engage in financial transactions without all financial records being made available to the Government by default.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

STATEMENT OF PUBLIC CITIZEN

215 Pennsylvania Avenue, SE • Washington, D.C. 20003 • 202/546-4996 • www.citizen.org

Testimony

Bartlett Collins Naylor

Public Citizen, Congress Watch Division

Crypto-currencies: What are They Good for?

Senate Banking Committee

July 27, 2021

On behalf of more than 500,000 members and supporters of Public Citizen, we offer the following testimony for the Senate Banking Committee hearing titled, "Crypto-currencies: What are They Good for?"

Broadly, we believe that digital assets in the form of cryptocurrencies fail to constitute an efficient, available form of payment; represent a serious danger to investors; and harm the environment. We do support federal bank regulators exploring ways to streamline the payment systems, which might include federal sponsorship of a digital coin.

Payment System

The nation's financial payment system works for many Americans. Employees receive paychecks that are typically deposited, often electronically, into a bank account. These accounts can then be accessed for payments by way of checks, credit or debit cards, or through a withdrawal of cash. There are roughly $2 trillion in U.S. coins and notes now in circulation, although most of this circulates outside the United States. (The 60 percent estimated to circulate outside the United States is due to many reasons, including the fact that some countries use the US dollar as their own currency.)[1] But there is about $17

[1] *Monetary Base, Currency in Circulation*, FEDERAL RESERVE BANK OF ST LOUIS, (April, 2021) https://fred.stlouisfed.org/series/MBCURRCIR. J.P. Koning, *How Much U.S. Currency is Held Overseas?*,

trillion in deposits where transactions take place as accounting ledger notations, with no physical transfer of any item, such as cash.[2] The payment system can be convenient for many. One can purchase an item with as little cost as a candy bar with a credit card. The vendor receives payment in a matter of days. The buyer pays off the credit purchases monthly, and, with auto-pay, the credit card balance can be remitted with no further action by the customer.

But the payment system also contains serious flaws. Many U.S. residents lack a bank account. More than six percent of American households, or some 33 million citizens are without a traditional bank account. Some do not trust banks, while others lack the funds that financial institutions require to open and maintain an account.[3]

Even for those lucky people with deposit accounts, the payment system is slow. Overdraft fees can be substantial. Checks and credit card payments can take two days or more to clear, meaning that vendors are without these funds during that time. It is also costly. Checks and particularly wire transfers can include substantial fees. Banks charge interchange fees for credit cards, a substantial burden for retailers.[4] And it is complex, with thousands of banks with idiosyncratic ledger systems communicating with one another and the Federal Reserve.

There are also deposit substitutes outside the traditional banking industry, such as money market mutual funds, and repurchase agreements between institutional investors. During the 2008 financial crisis, breakdowns in these two areas led the Federal Reserve to engage in a major bailout to sustain some stability just so large institutions could meet their payrolls.[5]

Crypto-currencies

For some, digital assets or "crypto-currencies" promise a better payment system. With a digital asset kept on a decentralized ledger, the number of intermediaries would be reduced. Relatedly, there would be no intermediary assessing a fee on these transactions.

In the current landscape, this promise is proving illusory.

Most immediately, the prevailing crypto-currencies are gyrating wildly in price. Bitcoin, which is the largest such currency, changes value daily, sometimes by substantial percentages. During the three-month period ending in June 2021, Bitcoin traded as high as $60,000 per token and as low as $35,000.[6] A customer who believed that Bitcoin would rise in value would not rationally use one for a purchase on that day since they would be over-paying. They would only use the coin if they thought the price would fall. Conversely, a vendor who believed Bitcoin would fall would not accept the coin, since it would be an

---

BULLIONSTAR (Jul. 3, 2019) https://www.bullionstar.com/blogs/jp-koning/how-much-u-s-currency-is-held-overseas/

[2] Deposits, *All Commercial Banks*, FEDERAL RESERVE BANK OF ST LOUIS, (June 4, 2021) https://fred.stlouisfed.org/series/DPSACBW027SBOG

[3] Mehrsa Baradaran, *How the Other Half Banks*, HARVARD UNIVERSITY PRESS (2015) https://www.hup.harvard.edu/catalog.php?isbn=9780674983960

[4] Aaron Klein, *A Few Small Banks Have Become Overdraft Giants*, BROOKINGS INST. (Mar. 1, 2021) https://www.brookings.edu/opinions/a-few-small-banks-have-become-overdraft-giants/

[5] Mary Shapiro, *Perspectives on Money Market Mutual Fund Reform,* SECURITIES AND EXCHANGE COMMISSION (June 21, 2012) https://www.sec.gov/news/testimony/2012-ts062112mlshtm

[6] *Bitcoin,* COINDESK (website accessed June 11, 2021) https://www.coindesk.com/price/bitcoin

underpayment, and would only accept the token if they believed the price would rise. In other words, a gyrating price stifles the use of Bitcoin as a vehicle of market exchange.

Second, the promise of cost-free transactions has also proven illusory. The cost of transactions for Bitcoin are substantial and vary greatly. In the last year, they have reached $300 for each transaction.[7] Related to this, the same population that lacks a bank account, and who are most sensitive to financial fees, may also lack the technology assets to interact with digital currencies.

Third, the number of crypto-currencies is staggering, and growing. By one estimate, as of April 2021, there were more than 10,000 different cryptocurrencies.[8] That is a greater than the number of banks in the United States. One of these, namely Dogecoin, was created as a "joke," according to its founders.[9] The total dollar value of this universe is around $2 trillion, but that amount itself swings substantially. Bitcoin's total value is the largest, at about $700 billion. Ethereum is the second largest at about $288 billion. The 100th largest is Ravencoin, with a market capitalization of $640 million. The 200th largest is Travala.com, at $135 million.[10] With 10,000 separate crypto-currencies, it appears unfathomable how customers and vendors can agree on which one to use. A few retailers have experimented with accepting Bitcoin for payment, but many have stopped.[11]

Fourth, the claim that crypto-currency cannot be stolen has proven untrue. While it may not be as vulnerable to street theft as cash may be, or to cyber criminals hacking a bank account, a cyber-criminal might be able to hack into a personal computer where bitcoin codes are kept. Recently, a ransom paid by Colonial Pipeline to hackers that took over their system (which led to a temporary decline in gasoline supplies on the East Coast), was recovered by the FBI. Reported the *Wall Street Journal*, "Crypto experts say it is at times easier to track than hard currencies such as U.S. dollars."[12]

Investments

To date, crypto currencies are viewed mainly as a speculative investment. As with their use in the payment system, we believe this arena is perilous and FDIC-insured institutions should not abet investment. Banks are and should be intermediaries between savers and users of capital. Workers can deposit their paychecks in banks, and those funds can be used to grant loans to individuals, in the form of mortgages or other loans, or to businesses for growth. Businesses that grow large enough might eventually tap the broader capital markets, such as through an initial public offering of stock. The investor in that stock is purchasing a share of the company, a claim on the future profits of that enterprise. The stock investor owns something real, a company that produces real goods and services.

---

[7] *Bitcoin Average Cost Per Transaction,* YCHARTS (website accessed June 11, 2021) https://ycharts.com/indicators/bitcoin_average_cost_per_transaction

[8] *Understanding the Different Types of Cryptocurrencies,* SOFI LEARN (Jan. 15, 2021) https://www.sofi.com/learn/content/understanding-the-different-types-of-cryptocurrency/

[9] Avi Salzman, *Dogecoin Was Started as a Joke,* BARRONS (May 5, 2021) https://www.barrons.com/articles/dogecoin-started-as-a-joke-now-its-too-important-to-laugh-off-51620229273

[10] *All Cryptocurrencies,* COINMARKETCAP (website accessed June 11, 2021) https://coinmarketcap.com/all/views/all/

[11] Steve Fiorillo, *How to Use Bitcoin for Purchases,* THE STREET (April 18, 2018) https://www.thestreet.com/investing/what-can-you-buy-with-bitcoin-14556706

[12] James Uberti, *How the FBI Got Colonial Pipeline's Money Back*, WALL STREET JOURNAL (June 11, 2021) https://www.wsj.com/articles/how-the-fbi-got-colonial-pipelines-ransom-money-back-11623403981

The 10,000 crypto-currencies, by contrast, are simply computer creations with no promise of income, no real assets, no services attached to them.

Many investment professionals share a similar view. Berkshire Hathaway CEO Warren Buffett recently called crypto-currency "rat poison squared." His associate Charlie Munger labelled trading in this market as "dementia."[13] Investor Mark Cuban said he'd prefer bananas to bitcoin, "Because at least as food, bananas have intrinsic value."[14] JPMorgan CEO Jamie Dimon said he'd fire any employee he found investing in Bitcoin. Other skeptics include Allianz economist Mohamad El-Erian, economist Paul Krugman, and Oaktree Capital Management founder Howard Marks. [15]

If crypto-currencies are not a viable substitute for the payment system, why should anyone consider them a viable investment? The sad reality is that about 46 million Americans now own Bitcoin alone.[16] Why do so many people invest in Bitcoin and other cryptocurrencies? We assume, as with a stock or other traditional asset, these speculators believe the price will rise and that they will profit. To date, that has been the case. Crypto-currency did not exist two decades ago and is now worth a collective $2 trillion, as previously noted. That's four times the market capitalization of JP Morgan.[17] Speculators who purchased at lower prices are, indeed, sitting on a profit. Bitcoin sold for $1,000 in 2017, before peaking at $60,000 in 2021.[18] Would-be speculators saw these winnings and likely were attracted to the arena.

Bolstering the stories of success, mainstream institutions and public influencers are affirming the legitimacy of crypto-currencies as investments. Well known brokers, including large firms catering to small investors such as Schwab, now offer crypto-currencies. [19] Wells Fargo offers the product to is elite clients.[20] Crypto-currencies legitimized by large institutions naturally invites otherwise rational people to consider allocating at least some of their portfolio to this sector.

This is troubling because this collective $2 trillion is money that could otherwise be invested in real assets that would truly benefit the public. Currently in Congress, a bipartisan group of lawmakers are debating investment in the nation's infrastructure, and the dollar figures being discussed are less than that now tied up in crypto-currencies. Venture capitalists and other funders of entrepreneurs are always hungry for additional capital.

---

[13] James Royal, *Warren Buffet Says to Avoid these Two Types of Hot Investments,* BANKRATE (May 6, 2019) https://www.bankrate.com/investing/warren-buffett-says-avoid-these-hot-investments/

[14] Taylor Locke, *Mark Cuban: Bitcoin Is 'More Religion Than Solution' And Won't Help In 'Doomsday Scenarios,* CNBC (Dec. 17, 2020) https://www.cnbc.com/2020/12/17/mark-cuban-bitcoin-is-a-store-of-value-that-is-more-religion.html

[15] Trisha Phillips, *Bill Gates and Other Powerful People Who Hate (or Love) Bitcoin,* SHOWBIZ CHEATSHEET (MAY 25, 2018) https://www.cheatsheet.com/money-career/powerful-people-love-or-hate-bitcoin.html/

[16] *About 46 Million Americans Own Bitcoin,* NASDAQ (May 14, 2021) https://www.nasdaq.com/articles/about-46-million-americans-now-own-bitcoin-2021-05-14

[17] *JP Morgan,* YCHARTS (website accessed June 11, 2021) https://ycharts.com/companies/JPM/market_cap

[18] James Royal, *Best online brokers for buying and selling cryptocurrency in June 2021,* BANKRATE *(June 1, 2021) https://www.bankrate.com/investing/best-online-brokers-cryptocurrency-trading/*

[19] James Royal, *Best online brokers for buying and selling cryptocurrency in June 2021,* BANKRATE *(June 1, 2021) https://www.bankrate.com/investing/best-online-brokers-cryptocurrency-trading/*

[20] *Wells Fargo: US Bank Set to Offer Crypto to Rich Clients*, BBC (May 19, 2021) https://www.bbc.com/news/business-57147386

Meanwhile, investment scams involving cryptocurrencies abound. In a five month period ending March 2021, the Federal Trade Commission reported 7,000 cryptocurrency scams covering some $80 million in reported losses. That is 12 times the number of scams reported during the same period a year earlier, with a 1000 percent greater estimated loss.[21] Alexis Goldstein, financial policy director of the Open Markets Institute, reviewed some of these scams in testimony before the House Financial Services Subcommittee on Oversight and Investigations. For example, some malicious actors created digital coins that can be purchased but not sold. Others promise enormous returns that proved untrue. [22]

Cryptocurrencies also serve as a medium of payment for illicit activities, as noted in the Colonial Pipeline case above. One study found that "approximately one-quarter of Bitcoin users are involved in illegal activity" and that an estimated $76 billion in illegal activity per year involve bitcoin (46% of bitcoin transactions), "which is close to the scale of the U.S. and European markets for illegal drugs."[23]

As a steward of sound public policy, the FDIC should not abet the legitimization of crypto-currencies. As such, we urge the FDIC to oppose bank efforts to promote crypto-currencies with depository, investment or other services.

Energy and Climate Issues

Counterintuitively, the promise of friction free commerce through cryptocurrency without the need of paper documents coursing by way of vans and other transport through physical roads has also proven illusory. In fact, many cryptocurrencies are major energy users. Many cryptocurrencies are created through "proof-of-work" mining that involves using computers to solve useless mathematical puzzles in exchange for newly minted cryptocurrency tokens. This mining absorbs considerable amounts of electricity. Bitcoin miners alone annually use an estimated 130 Terawatt-hours, which is about 0.6 percent of world electricity consumption, according to one estimate.[24] At a time of climate change crisis, tapping our energy supply for specious cryptocurrency should not be promoted.

Central Bank Digital Currency

At the same time, Public Citizen does support exploration of a Central Bank Digital Currency (CBDC). This federal digital coin, in one form dubbed a FedAccount, holds the promise to address some of the problems with the payment system reviewed above. Currently, depository institutions maintain accounts with the Federal Reserve. The FedAccount would be available to ordinary citizens.

Conceived by Lev Menand of Columbia Law School in June 2018, the CBDC would be a Federal Reserve account. It would be available to "any U.S. resident or business in digital wallets operated by the Fed,

---

[21] Emma Fletcher, *Cryptocurrency Buzz Drives Record Investment Scam Losses,* FEDERAL TRADE COMMISSION (May 17, 2021) https://www.ftc.gov/news-events/blogs/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses

[22] Alexis Goldstein, *Testimony,* HOUSE FINANCIAL SERVICES COMMITTEE (June 20, 2021) https://financialservices.house.gov/uploadedfiles/hhrg-117-ba09-wstate-goldsteina-20210630-u1.pdf

[23] Sean Foley, et al, *Sex Drugs and Bitcoin*, THE REVIEW OF FINANCIAL ECONOMICS, (May 2019) https://academic.oup.com/rfs/article/32/5/1798/5427781

[24] *Cambridge Bitcoin Electricity Consumption Index*, UNIVERSITY OF CAMBRIDGE, (website visited July 1, 2021) https://cbeci.org/

the Post Office, or one of the country's several thousand community banks," he explains.[25] "The digital wallets would charge no fees and have no minimum balances. They would come with debit cards, direct deposit, and bill pay. They would have customer service, privacy safeguards, and fraud protection—if for example one lost their password. And these accounts would earn interest at the same rate that the Fed pays to banks."

Lack of profitability for the banks represents one of the reasons that banks fail to service roughly six percent of the population. The FedAccount would be available regardless of any balance. The FedAccount would be streamlined with immediate clearing. There would be no fees. With such an account, delivery of federal payments such as Covid relief or other government benefits, would be immediate.

Important questions must be answered. For example, many bank account holders are subject to garnishments because of unpaid debt. Debt collectors would have a simple way to garnish funds through the CBDC. That also means the Federal Reserve would need to engage with debt collectors in addition to individual Federal Reserve account holders. There may be political issues. For example, the CARES Act might have more effectively delivered needed rescue funds to needy Americans via FedAccount system. However, some of the individuals who received relief may have been subject to garnishment, meaning the Federal Reserve would be in a position of deciding whether, in times of extraordinary need, it would protect or release these funds. A similar issue applies to overdrafts, which means the Federal Reserve may need to institute a policy to ensure financially vulnerable individuals are not being harmed by unaffordable fees.

In conclusion, we thank the committee for exploring this important issue. The payment system fails to serve a significant portion of the population and we commend efforts to answer this deficiency such as exploration of a central bank digital currency. We also urge the full committee to continue its attention to the perils of privately sponsored crypto-currencies.

---

[25] Lev Menand, *Testimony*, U.S. SENATE BANKING COMMITTEE (June 9, 2021) https://www.banking.senate.gov/imo/media/doc/Menand%20Testimony%206-9-21.pdf