S. HRG. 115–453

EXPLORING THE CRYPTOCURRENCY AND BLOCKCHAIN ECOSYSTEM

HEARING

BEFORE THE

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

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

ON

EXPLORING THE OPPORTUNITIES AND CHALLENGES SURROUNDING THE CRYPTOCURRENCY AND BLOCKCHAIN ECOSYSTEM

OCTOBER 11, 2018

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

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

U.S. GOVERNMENT PUBLISHING OFFICE
34–525 PDF WASHINGTON : 2020

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

RICHARD C. SHELBY, Alabama
BOB CORKER, Tennessee
PATRICK J. TOOMEY, Pennsylvania
DEAN HELLER, Nevada
TIM SCOTT, South Carolina
BEN SASSE, Nebraska
TOM COTTON, Arkansas
MIKE ROUNDS, South Dakota
DAVID PERDUE, Georgia
THOM TILLIS, North Carolina
JOHN KENNEDY, Louisiana
JERRY MORAN, Kansas

SHERROD BROWN, Ohio
JACK REED, Rhode Island
ROBERT MENENDEZ, New Jersey
JON TESTER, Montana
MARK R. WARNER, Virginia
ELIZABETH WARREN, Massachusetts
HEIDI HEITKAMP, North Dakota
JOE DONNELLY, Indiana
BRIAN SCHATZ, Hawaii
CHRIS VAN HOLLEN, Maryland
CATHERINE CORTEZ MASTO, Nevada
DOUG JONES, Alabama

Gregg Richard, *Staff Director*
Mark Powden, *Democratic Staff Director*

Jonathan Gould, *Chief Counsel*
Kristine Johnson, *Economist*

Laura Swanson, *Democratic Deputy Staff Director*
Elisha Tuku, *Democratic Chief Counsel*
Corey Frayer, *Democratic Professional Staff Member*

Dawn Ratliff, *Chief Clerk*
Cameron Ricker, *Deputy Clerk*
Shelvin Simmons, *IT Director*
James Guiliano, *Hearing Clerk*
Jim Crowell, *Editor*

CONTENTS

THURSDAY, OCTOBER 11, 2018

WITNESSES

Additional Material Supplied for the Record

EXPLORING THE CRYPTOCURRENCY AND BLOCKCHAIN ECOSYSTEM

THURSDAY, OCTOBER 11, 2018

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

The Committee met at 10:01 a.m., in room SD–538, Dirksen Senate Office Building, Hon. Mike Crapo, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN MIKE CRAPO

Chairman CRAPO. This hearing will come to order.

Today the Committee will continue its exploration of the opportunities and challenges surrounding the cryptocurrency and blockchain ecosystem.

Prior to the introduction of Bitcoin and underlying blockchain ledger in 2009, there was no similar solution to the double-spend problem—where the same digital currency could be spent more than once—which did not require a third-party intermediary.

While Bitcoin, the first decentralized cryptocurrency, has been around for nearly a decade now, cryptocurrencies have gained particular attention in the past 2 years, due in part to their meteoric rise and subsequent fall in value last year.

Advancements since Bitcoin's creation have expanded blockchain's uses and given way to things like "Initial Coin Offerings," a method of crowdfunding that has become popular in the cryptocurrency community.

While the technologies underpinning cryptocurrencies have the ability to transform the composition of, and ability to access, capital and the financial system, much of the recent news about cryptocurrencies has been negative, focusing on enforcement actions, hacks on international exchanges, and concerns raised by various regulators and market participants.

To that end, in February of this year, the Committee held a hearing with the SEC and CFTC to examine their oversight roles of cryptocurrency-related products and activities under their respective jurisdictions.

Since that hearing, the agencies have made strides to provide further clarification on their thinking surrounding cryptocurrency-related issues. But some regulatory and oversight questions still remain.

The regulatory questions, price volatility, and reports of things like pump-and-dump schemes have raised a lot of questions surrounding the cryptocurrency and blockchain ecosystem that need to be better understood.

Blockchain networks have the potential to improve processes for things like smart contracts, payments and settlement, identity management, and even things yet undiscovered.

In order to move forward in a productive way and give these innovations the room to flourish and develop in a safe and sound way, we need to sort through the static and better understand what exactly are the opportunities and challenges facing this ecosystem.

For example, the Committee would benefit to hear about: the use of cryptocurrencies and derivative products as a store of value or medium of exchange or payment; the current and potential applications of blockchain technology; and the regulatory issues surrounding the various facets of the ecosystem and how they can be improved.

I look forward to hearing about this and other issues from our witnesses today.

Senator Brown.

OPENING STATEMENT OF SENATOR SHERROD BROWN

Senator BROWN. Thank you, Chairman Crapo, for holding this hearing. And thanks to the two witnesses. Mr. Van Valkenburgh, welcome, and, Dr. Roubini, welcome to the Committee.

Today's hearing happens to fall just shy of the tenth anniversary of Bitcoin and the blockchain being introduced to the world—October 31, 2008. We were in the midst of a global financial crisis. You cannot blame some Americans for hoping that an alternative banking system could be created that would be superior to the one in shambles at that time.

Bitcoin, and other cryptocurrencies like it, promised to make payments faster and easier and cheaper, and to eliminate our reliance on risky financial institutions whose failures harmed workers and families in all of our communities.

The last 10 years, unfortunately, have shown that misconduct, fraudulent investment schemes, and cybersecurity threats are not unique to the traditional financial system. When a cryptocurrency goes bust or a poorly supervised exchange fails, it is often hardworking Americans left holding the bag.

We want to see innovations in the financial system, innovations that help Americans keep more of their money by avoiding fees or that make it easier to borrow for a small business startup.

But so far, despite all the energy and investment dedicated to finding a use for the blockchain, there are few real-world applications and an alarming number of scams.

Cryptocurrency prices have swung wildly over the last year. Inexperienced investors who were hoping to get in on the next big financial innovation have seen the value of these investments fall by more than 75 percent from their peak.

Though they have raised billions of dollars from investors, few if any Initial Coin Offerings (ICOs) have registered with the SEC. Chair Clayton told this Committee in a February hearing, "Every Initial Coin Offering I have seen is a security."

Last month, the New York Attorney General released a report on several cryptocurrency trading platforms that pointed to evidence of widespread manipulation and identified several exchanges that do not follow “anti-money-laundering” or “know your customer” requirements.

With a decade of experience, much of the irrational exuberance around cryptocurrencies and blockchain technology has subsided, and we have an opportunity to set more realistic expectations for how these innovations might be used to promote a fairer and more competitive economy.

I hope this technology will prove useful, particularly in helping people who are unbanked or underserved by the traditional financial system. I understand why individuals might be interested in it. But at this point, it is easier to see the malign impacts on society as a whole than the constructive ones. That is why we look forward to your testimony.

Thank you. Chairman Crapo. Thank you, Senator Brown.

Today we are fortunate to have two witnesses from different perspectives whose in-depth knowledge of cryptocurrencies will be an asset to the community.

First we will hear testimony from Dr. Nouriel Roubini, Professor of Economics and International Business at NYU’s Stern School of Business. And then we will hear from Mr. Peter Van Valkenburgh, Director of Research at Research and Advocacy Group, Coin Center.

Dr. Roubini, you may proceed—oh, before you do, as I always do, I remind you to please try to pay attention to the clock and keep your initial remarks to 5 minutes. You will have opportunities to respond and add during questions. And I remind my colleagues of the same limitations that they have on their questioning time.

With that, Dr. Roubini, please proceed.

STATEMENT OF NOURIEL ROUBINI, PH.D., PROFESSOR OF ECONOMICS, STERN SCHOOL OF BUSINESS, NEW YORK UNIVERSITY

Mr. ROUBINI. Thank you. Chairman Crapo, Ranking Member Brown, and Members of the Committee, thank you for the opportunity to testify today on the topic of the cryptocurrency and blockchain ecosystem.

My name is Nouriel Roubini. I am a professor of economics at New York University. I am an expert of the global economy, of asset and credit bubbles, and of financial crises.

In summary, my views on this ecosystem are as follows:

First, crypto is the mother or father of all scams and bubbles, a bubble that has finally gone bust this year.

Second, blockchain is the most over-hyped technology ever, and it is no better than a glorified database.

Let me elaborate on these points.

First, a recent study showed that 81 percent of all ICOs were scams to begin with, 11 percent of them have been failing or are dead, and only 8 percent are still traded on exchanges.

Second, after a massive bubble in 2017, Bitcoin has fallen by 70 percent. This year, other major cryptocurrencies have fallen by 80 percent, and thousands of other ones have fallen by 95 percent.

This entire asset class is literally imploding now. Just yesterday, major cryptocurrencies plunged another 10 percent in a day.

Third, these assets are not currencies. Calling them "cryptocurrencies" is nonsense. They are not a unit of account. They are not a means of payment. They are not a stable store of value. Bitcoin can do only five transactions per second. Visa can do 25,000 per second. Nobody uses Bitcoin for transactions apart from criminals and terrorists. Cryptomining is also an environmental disaster as the system wastes massive amounts of energy.

Fourth, there is a revolution in financial services, but it has nothing to do with blockchain or crypto. It is called "FinTech," and it is based on a combination of AI, big data, and Internet of Things (IOT). And it is already being used daily by billions of people for billions of financial transactions. There is no blockchain in FinTech.

Fifth, the crypto-ideological utopia is a libertarian dream of full decentralization of all human transactions—no governments, no central banks, no corporation, no banks, no trusted institutions. It is totally utter nonsense.

Sixth, crypto-land is now subject to the opposite and dangerous trend: massive centralization. Mining is centralized and controlled by oligopolies in authoritarian countries like China and Russia. Trading has centralized 99 percent of all transactions occurring on nonsecure, centralized exchanges that are being hacked on a daily basis. Development is centralized as the technological elite is police, prosecutor, and judge. They arbitrarily change the code and "fork" coins into new ones when things go wrong. And wealth is massively concentrated in crypto-land. The Gini coefficient of inequality for Bitcoin is worse than North Korea. It is quite an achievement.

Seventh, there is massive price manipulation in crypto-land: widespread pump-and-dump schemes, spoofing, wash trading, insider trading. Coins like Tether that are created by fiat and used to manipulate upward prices. Massive criminality.

Eighth, ICOs associated with security tokens are noncompliant securities that break all security laws. They are mostly scams, and even the SEC created a fake website to warn investors of such initial coin scams.

Ninth, utility tokens and widespread tokenization would mean a return to the Stone Age of barter. Even the Flintstones knew better than crypto as they used clam shells as their own one currency.

Tenth and final point, corporate blockchain—so-called enterprise DLT—are glorified databases and they have nothing to do with blockchain. They are private rather than public. They are permissioned rather than permission-less. They are based on trusted authorities verifying transactions rather than being trustless. They are not distributed on millions of computers but, rather, on a few selected control ledgers or databases. They do not use cryptographic games or tend to get transactions but, rather, trusted permissioned authorities.

In summary, they claim to be blockchain, but they have nothing to do with blockchain. And 90 percent of all corporations experimenting with them have decided that they are no better than traditional databases, and since they are more costly and less efficient than databases, they will not use them. Only 1 percent of all CIOs say that there will be any adoption of DLT in their organizations, and 80 percent of all CIOs have no interest in this technology.

It is no wonder as no organization, government, corporation, or bank would ever want to put on a public, permission-less, distributed, trustless ledger all these transactions with customers and suppliers. It does not make sense, and it is not going to happen. So blockchain is a lot of hype and almost no reality, as an expert senior analyst recently concluded.

Thank you for your interest, and I am happy to answer any questions.

Chairman CRAPO. Thank you, Dr. Roubini.

Mr. Van Valkenburgh.

STATEMENT OF PETER VAN VALKENBURGH, DIRECTOR OF RESEARCH, COIN CENTER

Mr. VAN VALKENBURGH. Chairman Crapo, Ranking Member Brown, Members of the Committee, thank you for the opportunity to speak with you today. My name is Peter Van Valkenburgh, and I am the Director of Research at Coin Center, an independent nonprofit focused on the public policy issues affecting cryptocurrency and public blockchain networks.

What is Bitcoin? Bitcoin is the world's first cryptocurrency, and it works because of the world's first public blockchain network.

What does Bitcoin do? It is simple. It lets you send and receive value to and from anyone in the world using nothing more than a computer and an internet connection.

Now, why is it revolutionary? Because unlike every other tool for sending money over the internet, it works with the need to trust a middleman. The lack of any corporation in between means that Bitcoin is the world's first public digital payments infrastructure. And by "public," I simply mean available to all and not owned by any single entity.

Now, we have public infrastructure for information, for websites, for email. It is called the "Internet." But the only public payments infrastructure that we have is cash, as in paper money, and it only works in face-to-face transactions.

Before Bitcoin, if you wanted to pay someone remotely over the phone or the internet, then you could not use public infrastructure. You would rely on a private bank to open their books and add a ledger entry that debits you and credits the person you are paying. And if you both do not use the same bank, well, then there will be multiple banks and multiple ledger entries in between.

With Bitcoin, the ledger is the public blockchain, and anyone can add an entry to that ledger, transferring their bitcoins to someone else. And anyone, regardless of their nationality, race, religion, gender, sex, or creditworthiness, can for absolutely no cost create a Bitcoin address in order to receive payments digitally. Bitcoin is the world's first globally accessible public money.

Is it perfect? No. Neither was email when it was invented in 1972. Bitcoin is not the best money on every margin. It is not yet accepted everywhere. It is not used often to quote prices, and it is not always a stable store of value. But it is working, and the mere fact that it works without trusted intermediaries is amazing. It is a computer science breakthrough, and it will be as significant for freedom, prosperity, and human flourishing as the birth of the internet. And Bitcoin is just the beginning. If we can replace private payments infrastructure, then we can replace other private choke points to human interaction as well.

Now, why should we want to build more public infrastructure? Why should we embrace blockchains over corporate intermediaries? Why should we tolerate their inefficiencies and work to make them better? Why should we want the pioneers of this technology here in the United States and not fleeing overseas? A simple reason: Because the corporate intermediaries providing today's critical but privately owned infrastructure are becoming fewer, larger, and more powerful, and their failures are increasingly grave.

So roughly half of all Americans, 143 million people, had their Social Security numbers exposed to hackers because of a breach at Equifax. The SWIFT network has relayed hundreds of millions of dollars in fraudulent transactions because of hacked member banks in Bangladesh, Vietnam, Ecuador, and Russia. The FBI suspects now that the largest of these hacks was perpetrated by North Korea.

Corrupt, low-level employees at an Indian bank, Punjab National, were able to fraudulently certify SWIFT messages, stealing $1.8 billion. It is the largest electronic bank robbery in history. In fact, it is the largest bank robbery in history.

In October 2016, an estimated 1.2 million internet-connected devices were hacked and turned into a botnet that for several hours made prominent websites unavailable across Europe and North America, including CNN and Fox News, the New York Times and the Wall Street Journal.

Increasingly, physical machines are being connected to the internet to augment their capabilities. They are wired through servers that are owned and maintained by private and trusted intermediaries—the so-called Internet of Things. Pacemakers from St. Jude's Hospital have been hacked, baby monitors from TRENDnet have been hacked, and jeeps from Jeep have been hacked to the point where they can be remotely commandeered and driven off the road.

Now, those vulnerabilities are inescapable in systems that have single points of failure. It does not matter if the point of failure is a corporation or if it is a government. There should not be a single point of failure. Similar choke points existed before the internet. If you wanted to deliver a message, you would have to go through one of three television broadcasters or a handful of newspapers. Private corporations are essential, but no critical infrastructure should rely on one or two. The internet removed single points of failure in communications infrastructure and ushered in a wave of competition among new media corporations building on top of its public rails.

Blockchains can similarly disintermediate critical payments and IOT infrastructure. The technology is not yet ready to answer all of those questions today, but it is our best hope. And as with the internet in the 1990s, we need a light touch, pro-innovation policy to ensure that these innovations flourish in America for the benefit and security of all Americans.

Thank you, and I look forward to your questions.

CHAIRMAN CRAPO. Thank you, Mr. Van Valkenburgh. And I would like to start with you. Your testimony details three particular areas where decentralized computing can be useful and helpful: electronic cash, identity, and the Internet of Things. Some use cases like Bitcoin already exist, while others are conceptual. Cryptocurrencies like Bitcoin have experienced volatile price fluctuation over the past year.

I am going to ask you first and then, Dr. Roubini, I will ask you to comment on this as well. Where do you see things going in the next year or so? Under what conditions do you see market value stabilizing?

Mr. VAN VALKENBURGH. Thank you, Chairman Crapo. Much of the ongoing volatility that we are seeing I think stems from a struggle to find a level for something brand new. So when tulips were first introduced to the Netherlands from Arabia and they became very popular amongst the rich set, it was hard to find a price, and a lot of irrational exuberance pervaded those markets. We saw volatility in equity markets when trading joint stock companies became a new phenomenon, the South Sea and Mississippi bubble. And we saw volatility in the dot-com companies when the internet was brand new. Finding a level is very difficult.

Fortunately, we are now beginning to see institutional investment coming online with respect to Bitcoin and eventually other cryptocurrencies as well. We have got CFTC-regulated Bitcoin derivatives markets, and that means that we will have, I think, better sell side research from the institutional investment class, and there will be the possibility for people to take short positions and rationalize the market.

Now, key to this effort is more institutional grade products that are regulated by the proper authorities. So we have CFTC-related derivatives. We could use ETFs regulated by the SEC where there is institutional-grade custody and where there are known accounting standards and where purchasers know where they stand.

We could also use better custodians in general. Comptroller Otting at the Office of the Comptroller of the Currency has revitalized the process of offering FinTech charters to new companies offering new services that do not look like traditional banks. A nationally chartered bank that custodies cryptocurrency is something that I think would bring more rationality to these markets.

Chairman CRAPO. Thank you.

Dr. Roubini, would you comment on the same issue?

Mr. ROUBINI. Yes, cryptocurrencies are not scalable, are centralized, they are not decentralized, and they are not secure. Bitcoin is five transactions per second, and there is a massive concentration of the mining among, about half of those are the Chinese, Russian, and others' miners. So you say you do not rely on trends at institutions. You are relying on an oligopoly of individuals that are shady in countries that you have no control.

There are solutions that claim that in the future are going to be scalable, but the only way they achieve scalability, like proof of stake, is going to lead to even more cartelization of mining. Once you have cartelization of mining, there is no security. If I lose my credit card or somebody steals my bank account, I call and it is blocked. I have deposit insurance. I have lender of last resort support of the financial system. Yes, I pay a fee. If somebody is hacking your crypto wealth, it is gone forever, no deposit insurance, no lender of last resort, no solution on the immutable hacking of your wealth. There is no security in this space, there is no scalability in this space, and there is massive centralization that is very risky, and it is not going to change.

Chairman CRAPO. Well, thank you. I only have about a minute left, so as a follow-up, many of the projects or use cases for decentralized computing, as Mr. Van Valkenburgh's testimony refers to it, are still in the conceptual phase or are not being widely adopted as of yet. Are there particular factors hindering implementation or adoption of blockchain or decentralized computing solutions? And what are the most meaningful steps that market participants or regulators can take to create certainty or promote a safe path forward? I would like you each to take about 30 seconds to answer me, please.

Mr. VAN VALKENBURGH. So decentralized computing-use cases are hard challenges. As I said, email was invented in 1972, and it took 20 years for those systems to be friendly enough for consumers to want to use them to send messages. We have got choke points that are vulnerable on the internet today that could be made better with blockchains. For one, the DNS system, which was the hack that brought the websites and made them unavailable, the New York Times and——

Chairman CRAPO. I will have to stop you there and go to Dr. Roubini.

Mr. ROUBINI. Well, there is no government or corporation or bank that is going to use a public, decentralized, permission-less system. It will be very risky to let millions of computers somewhere in China verify your transaction. Therefore, all enterprise DLT is private, is permission, is based on trust. So the idea of decentralization is never going to fly. Ask any corporation or any bank. No one of them is going to go to a decentralized system. It is nonsense.

Chairman CRAPO. Thank you.

Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

Dr. Roubini, let us assume blockchain technology and some cryptocurrencies overcome the issues that you raise in your testimonies. Are there applications that could be beneficial on a broad scale to address problems in the financial sector?

Mr. ROUBINI. Well, I do believe that there is some innovation. As I pointed out, if you are talking about enterprise DLT or corporate blockchains, the systems that are private, they are permissioned, they are not distributed, they have trusted authority to authorize transactions, and in my view these are just glorified databases. They are being called "blockchain," but they are not, and we can improve the efficiency of source of a transaction, financial and corporate, by having an integration of databases to reduce the transaction cost. But I do not think that we are going to go to a solution that is based on a public, permission-less, and trustless system. Nobody is going to accept it, no government, no corporation, or no bank.

So there is lots of work we can do of improving, and as I pointed out, the revolution in FinTech that is going to lead to banking services to the poor and unbanked is a revolution, is a revolutionizing payment system, credit allocation, insurance, asset management, capital transactions. It has nothing to do with blockchain. You have AliPay and WeChat Pay in China. We have Venmo, Square, PayPal in the United States. We have UPI systems in India. We have M–Pesa used by poor farmers in Kenya and all over Africa. Billions of transactions done by billions of people every day. That is the FinTech revolution.

What is the penetration of blockchain after a decade? Twenty-two million users and half of them are not using it. After a decade of the internet, with 1 billion users, the penetration of blockchain and crypto is collapsing. You have falling users, collapse of 80 percent of transactions, and transaction costs as a share of transaction have gone through the roof. It is the opposite of any successful technology in the financial sector or the internet. It is just the opposite.

Senator BROWN. Thank you.

Mr. Van Valkenburgh, it is one thing for tech billionaires or the Winklevoss twins to be investing in a complex and poorly regulated market, but I am concerned about families who risk their savings. What is the profile of the average person who is investing in this market, whether it is Bitcoin or buying into ICOs and other unestablished technologies?

Mr. VAN VALKENBURGH. So the profile of your average investor is technologically sophisticated because you have to deal with things like private and public keys or at least understand how the company that you are working with is securing them if it is coin base or some other exchange. And it is usually younger people who are interested in these new alternatives, perhaps because they feel like the legacy financial system has in some ways disappointed them, and they are looking for alternatives, I think in good faith.

Now, that said, are they safe? Are they being protected? Are there good regulations in place? Exchanges in the United States are regulated by the Federal Government for anti-money-laundering purposes, so FinCEN was one of the first out of the gate. America led here, and the rest of the world needs to catch up. FinCEN said exchanges are money services businesses, we need KYC, we need suspicion activity reporting.

From a consumer protection standpoint, though, they are regulated by the States. You have to get a money transmission license in every State where you have customers, assuming the State regulator for money transmission licensing has opined on the question of whether cryptocurrency exchanges fit their definition of money transmission or do not.

That regime is not entirely rational. These are natively global payments networks, and you are going State by State to get licenses from the proper authorities. And you are going to have 53 or so criminal background checks. The next one is not going to make you more or less secure for your customers.

Also, money transmission licensing regimes, they look for custody risk, which is important to safeguard against. But they do not deal in other investor protection concerns like manipulation and transparency in markets. I think it is about time that we had a serious policy conversation in this country about whether that State-by-State approach is reasonable and whether it is the best way to protect consumers. Federal preemption and an alternative Federal license for these companies, perhaps one that also polices from market manipulation and supervises for that, would be, I think, a wise choice that would make America a leader and protect our consumers.

Senator BROWN. Thank you.

Chairman CRAPO. Senator Kennedy.

Senator KENNEDY. Thank you, Mr. Chairman. Thank you, gentlemen.

Professor—well, let me reverse this. Mr. Van Valkenburgh, how long has cryptocurrency and blockchain technology been in existence?

Mr. VAN VALKENBURGH. That is an excellent question. So cryptocurrency and public blockchain networks have been around since 2008, 2009, when Satoshi Nakamoto invented them. But the blockchain that Mr. Roubini has described, the permissioned one, that has been around since the 1980s. It is actually older than I am. It is not a particularly innovative technology. It is just an Excel spread sheet. I think we actually in most cases agree on that point.

Senator KENNEDY. Let me interrupt you. Let us say 10 years. How is our world better off as a result of blockchain technology and cryptocurrency? Briefly.

Mr. VAN VALKENBURGH. So right now it is mostly anecdotal, quite frankly, because these things are not used widely, just as email was not used widely in the 1970s and 1980s until the 1990s. We have got a long runway. But, briefly, I have one example.

So the World Bank has found that in developing economies women are 20 percent likely to have a financial account at a bank, and accounts under their names are often controlled by their male relatives. There is a woman in Afghanistan, Roya Mahboob, who was a leading tech entrepreneur and wanted to pay her employees, most of whom were female coders. In order to get around this issue where she was unable to pay her female employees or their husbands were actually confiscating their money, she paid them using Bitcoin.

Senator KENNEDY. OK. I see your point.

Professor, how do you think, if at all, the world is better off as a result of us separating into cryptocurrency and in blockchain technology?

Mr. ROUBINI. I do not think the world is better off. There is a significant need for improving financial services, and as I pointed out, there is a revolution in financial services called "FinTech" based on AI and big data and so on, and it is used legally by billions of people, especially digital payment systems that are already available right now. They are low cost, they are efficient. They are used literally by billions of people all over the world, including billions of people even in Africa. That is really revolutionizing. If you are a poor farmer in Kenya, use M–Pesa. You can make a payment system. You can buy and sell your goods. You can get micro credit. You can do everything at very, very low cost, and these technologies are spreading everywhere. If you go to crypto, five transactions per second. You cannot do anything. You cannot be scaled.

Senator KENNEDY. That is what I want to ask you about. Let us set aside the Initial Coin Offerings and Bitcoin and all that. Let us talk about blockchain technology. You do not see any potential there?

Mr. ROUBINI. As I said, the only applications that are going to be acceptable by any private or public institutions cannot be based on a decentralized, permission-less, trustless system. Today there is no decentralization. The mining is controlled by a bunch of people in China, Belarus, Georgia, and Russia. And this is not a system that you want. There is a whole paper by a scholar at Princeton University showing there is a threat coming from China to Bitcoin because 75 percent of all mining of bitcoin is in China, and they are going to start to use it to manipulate at their own will. Therefore, do we want to rely on a private system? Yes. Do we want to rely on trusted permissions? Yes. Do we want to rely on a system that is kept private and safe? Yes. But it has nothing to do with blockchain. Blockchain means that you are relying on a cryptographic game where hundreds of thousands of computers verify transactions. There is no institution that is going to ever do that. So the solutions are back to basics.

Senator KENNEDY. Let me let Mr. Van Valkenburgh answer that, too.

Mr. VAN VALKENBURGH. So Mr. Roubini has brought up FinTech. He has brought up WePay and AliPay, which are innovations in China that are bringing lots of people into the financial system. It is important to point out that those are extremely large databases, and every Chinese citizen ends up with their full transaction history unencrypted in those databases, and the Chinese government, quite openly, has said that they can look at every financial record of every citizen in their country because of that FinTech innovation. That is a single point of failure in multiple regards. Those databases get hacked. Then those transactions are public to the world. But it is also a single point of failure in the fact that it is effectively government control and total surveillance over the population and every financial interaction they make in the world. It is a tool for totalitarians.

Senator KENNEDY. Thank you, gentlemen. Very interesting.

Senator BROWN. [Presiding.] Senator Jones.

Senator JONES. Thank you, Senator Brown. Thank you both for being here today. This is just an area that I am still learning a lot, and I want to move a little bit away from the financial markets per se, as I think most people—I am an old prosecutor, and I am concerned as much as anything with regard to the law enforcement aspect of this.

One thing that I learned as a prosecutor and as a lawyer is it seems like the bad guys are always two, three, or a dozen steps ahead of emerging technologies. I have learned as a Senator in looking at nations like Russia and China and North Korea that they also seem to be way ahead of the game when it comes to cybersecurity and those issues.

So my question is just really generic for both of you, and I will start with you, Mr. Van Valkenburgh. Talk to me a little bit about the dangers of cryptocurrency as it pertains to law enforcement, money laundering, human trafficking, drugs, the whole 9 yards in which emerging technologies can be exploited by the bad guys to really wreak havoc in our systems. Let us talk about that a little bit, and if you could address briefly, you know, what we can do in this early stage to try to prevent that. And then I will go to you, Mr. Roubini. I would like to just focus on those two as my questions.

Mr. VAN VALKENBURGH. Thank you, Senator Jones. You are absolutely right. Criminals are usually the earliest adopters of new technologies. In fact, I think if criminals are not using your technology, your technology is not worth anything.

Senator JONES. Good point.

Mr. VAN VALKENBURGH. So, you know, stock car racing and souped-up cars, ultimately NASCAR, was a phenomenon that was born out of bootleggers outrunning the cops during Prohibition. Technological innovation and ultimately something not so bad, but moments of disruption and things we need to worry about.

Now, with Bitcoin I think it is actually a positive story, especially here in the United States. As I said, FinCEN, our financial surveillance regulator, was fast out of the gate globally, first out of the gate to say that cryptocurrency exchanges need to know their customers and need to do suspicious activity reporting. So when you are getting onto the Bitcoin network by buying bitcoins in an exchange, your name is going to be taken down if you are buying at a U.S. exchange.

Now, what about transactions within the Bitcoin network that are not in an exchange? Well, they are public, on the public ledger that I have been talking about, and we have phenomenal law enforcement in this country that I have had the pleasure of meeting who have become extremely adept at analyzing that big data and finding and de-anonymizing or identifying a Bitcoin address as belonging to somebody involved in moving the proceeds of crime. I have even talked to folks who have said that they now prefer working cases where the illicit funds are moving through the Bitcoin network rather than calling up five or six international correspondent banks that do not keep good records or have shell accounts. There is one record to query, and it is perfect. If it was not, it would not work.

Senator JONES. All right. Mr. Roubini?

Mr. ROUBINI. Senator, you are absolutely right. Cryptocurrencies and blockchain have been used by criminals, by terrorists, by human traffickers, by tax evaders, just to engage in a variety of criminal activities. It is correct that, in principle, law enforcement authorities can go after this stuff. You know, the Silk Road was using Bitcoin for lots of transactions. They cracked it, and then they got arrested and prosecuted. But, of course, a system that in principle is supposed to be anonymous—and not just anonymous at the domestic level but globally—implies significant risk to enforcement.

Steve Mnuchin, Secretary of the Treasury, said we cannot allow Bitcoin and cryptocurrencies to become the next Swiss bank account. We have spent the last 20 years at the G–20 level to try to crack down on offshore financial centers, and now you have a tool that would allow anybody not to declare their income, not to declare their wealth, not to declare their capital gains. It is not going to be acceptable. Are we going to really go and find a system so that everybody is registered and everybody has to declare their income, their wealth, their capital gains, and their taxes? We are very far away from it, let alone other types of criminal activity.

Senator JONES. Did you want to respond real quick?

Mr. VAN VALKENBURGH. I did want to touch on one point.

Senator JONES. Still quick, because I have 30 seconds.

Mr. VAN VALKENBURGH. Steve Mnuchin's point was that the United States has pioneered the policy here, that we have classified exchanges as money services businesses and we require information from them. He was saying we do not want the rest of the world to not follow suit. His reference to Swiss banks was basically to say, "Hey, Switzerland, you should follow our lead."

Senator JONES. All right. Well, thank you both. And, you know, just for reference, Mr. Van Valkenburgh, I am headed to the NASCAR race in Talladega this weekend. I will make sure they are not running moonshine around the track.

[Laughter.]

Mr. VAN VALKENBURGH. Not too much moonshine, Senator.

Senator JONES. Thank you.

Senator BROWN. Senator Toomey.

Senator TOOMEY. Thank you, Senator Brown. Thanks to both of you for being here. This is a very helpful discussion.

It seems to me ICOs have featured some incredible scams. There are some that are very obvious. The volatility of Bitcoin has been breathtaking.

On the other hand, central banks over time have not had the greatest record of preserving the value of the meeting exchange that they are responsible for. We have discussed the friction in the payment systems that we have now, and I think FinTech is offering fabulous new ways to minimize that friction. But there will always be some friction, and even if they become extremely efficient, which they are, the payment system will still be in a fiat currency everywhere.

Dr. Roubini, you point out that bitcoin, for instance, is not really a unit of account, it is not a medium of exchange, and it is not a store of value. And I think that is true, but it did strike me that those are all issues of scale. Anything can be a currency if it is acceptable to enough people. It then takes on those characteristics.

What I think I hear you saying is that it is simply intrinsic to the nature of the underlying technology that it is fundamentally not scalable, that it cannot become widely enough used to achieve those characteristics that we normally use to define a currency. And that is what I am trying to understand. Why is it intrinsically—unless you disagree and that there is a different reason, but I thought I understood you to be suggesting that it just intrinsically cannot be scaled. Is that right?

Mr. ROUBINI. Yes. Some of it is quite technical, but Vitalik Buterin who invented the theorem called "impossibility trinity" that says in blockchain you cannot have at the same time scalability, decentralization, and security. So proof of work that is the one that Bitcoin is based is not scalable, only five transactions per second. You could say it is decentralized in principle, but it is not decentralized because 80 percent of the mining is done by six oligopolies. And once a situation of this sort is centralized, it is not secure.

Now, there are dozens of other consensus mechanisms that people are working in order to make it scalable.

Senator TOOMEY. OK, let me just—I just want to explore a couple of these things a little bit more, and let me give Mr. Van Valkenburgh a chance to respond.

First of all, is Bitcoin forever limited to five transactions per second, or is there any way to expand that scale? And, second, does an oligopoly on mining really matter? My understanding is there is ultimately a finite number of bitcoins that can be mined. And does it matter who mines them?

Mr. VAN VALKENBURGH. Thank you, Senator Toomey.

First of all, five transactions per second, we can do a lot more. There are multiple layers being built on top of Bitcoin today that do effectively things like batch settlement. So in just one or two transactions to the blockchain, you could have thousands of transactions.

Now, that sounds like we are reinventing the correspondent banking system and adding more centralized trust into it. It is not quite that. That is because the batch settlement can be done by a robot. Bitcoin is digitally native, so you can have smart contracts that manipulate and batch transactions together.

We have an M&M machine in our office. You would normally press a button and an M&M would come out. We have rigged it to work with lightning network payments, which are these second-level solutions, such that you can pay per the M&M with a fee that is about 0.002 cents, an incredibly negligible fee. If we can run transactions like that in a test net or in early days of a new layer, we can do all kinds of transactions per second.

On the question of Vitalik Buterin's trilemma, it is not an impossibility theorem. It is a trilemma. It is true. It is hard to have scale and decentralization and integrity of the data. Vitalik himself said it is not impossible. It is just a problem worth striving for. It is the kind of thing that American innovators and entrepreneurs should be working on.

Senator TOOMEY. Very quickly, does it matter that there is an oligopoly on the mining?

Mr. VAN VALKENBURGH. That is an excellent question. So it is worth asking, once you have a lot of mining power, what harm can you do? The Bitcoin protocol is decentralized not because it distributes power but because it checks power. What can a powerful person do to a weak person in the system? Bitcoin pits ambition against ambition, like our Federalist system here in the United States. And what I would say is you cannot do much. You cannot change the number of bitcoins in circulation. You would not be able to make that block and have it accepted by the network. You cannot reallocate or move other people's funds on the blockchain. The worst you can do is during the time when you have leveraged massive and costly resources, you can slow down the network and block transactions. It is a denial-of-service attack, something that all internet systems are vulnerable to, even the FinTech that Dr. Roubini talks about.

Senator TOOMEY. Thank you very much.

Senator BROWN. Senator Warren.

Senator WARREN. Thank you, Mr. Chair.

So virtual currencies are an interesting innovation that at least theoretically could provide benefits to consumers. But they also at the same time could empower scammers and criminals, and the challenge here, I think, is for us to try to figure out how to nurture the productive uses of virtual currencies while protecting consumers from scammers and other sorts of threats.

Now, one argument I often hear is that cryptocurrencies are decentralized, that anyone can mine new currency, unlike our current system, which relies on a central bank to perform that function.

Dr. Roubini, I know you are a skeptic of that claim. Could you just say a word about why?

Mr. ROUBINI. First of all, I am in favor of digital payment systems, but we can have digital payment systems without having cryptocurrencies. And as I pointed out, in the United States, in China, in India, in Africa, in Europe, there are tons of digital payment systems that do billions of transactions every day, they are used by billions of people, at low cost. So it is not the question of being in favor of only cash or a digital payment system. The FinTech allows you to do that. In the case——

Senator WARREN. No, I understand that. The question I am asking about is about decentralization, the claim that cryptocurrencies have the benefit because they are decentralized, and I said you are skeptic of that.

Mr. ROUBINI. It is false. The miners are all centralized, and it is a problem because, one, you can have 51 percent attacks, and those kind of attacks have occurred every day on smaller cryptocurrencies. So you can steal the money, and it is gone forever, those of such attacks. And people say, well, if you do it on Bitcoin, you are destroying Bitcoin. But if you have an oligopoly, what does an oligopoly do? They increase the prices, increase their margins of profit. If you look at the transaction costs in the space, they have gone through the roof as miners get their share of transaction. In the last year, they have gone up by 200 percent because they are using that oligopoly power to impose higher fees. It is an oligopoly. That is why it is inefficient.

Senator WARREN. So let me ask you the question then about the consequence of this concentration that you see. Is that inherent in the cryptocurrency or is it something that Government could do something about?

Mr. ROUBINI. It is inherent because there are economies of scale in mining, and these economies of scale that are in proof of work become worse once we get to scalable systems like proof of stake where whoever has a greater stake to begin with can do more of the mining. So there is massive concentration already in proof of work. People say that is not scalable, we are going to move to proof of stake. The proof of stake is going to become an even more concentrated cartel by definition of the system. You need massive mining factories all over China or Iceland to do the scale of transaction. You cannot do it on a laptop. That is why you lead to concentration in oligopolies.

Senator WARREN. OK. So you are saying it is inherent here. You know, these new technologies create these new opportunities, but if we are not careful, they can follow the same old patterns of they make the rich richer and they leave everybody else behind.

I want to ask about another one, and we will see if we can get these together because I want to ask Mr. Van Valkenburgh, according to reports, more than $1.1 billion of cryptocurrency was stolen in the first half of 2018. Why is cryptocurrency so easy to steal? And what should we be thinking about to secure it?

Mr. VAN VALKENBURGH. So those thefts were primarily with regard to newer cryptocurrencies who had experienced massive price increases and were being secured by exchanges or businesses, usually overseas, who did not scale their security in line with the value that was rising. That was a speculative bubble. I would not disagree with Dr. Roubini at all on that account. That was irrational, and it was triggered by this ICO market, which is largely fraud or unregistered securities issuance, which is, of course, not permitted.

So Bitcoin was not involved in the majority of the amounts that you are talking about there. It was these smaller currencies.

Senator WARREN. You know, I worry, though, because a lot of small investors get into the virtual currency market through Initial Coin Offerings, or ICOs, which allow companies to raise money by creating and selling these new virtual currencies. And you have just described a huge bubble around one of these.

In 2017, companies raised more than $6 billion using ICOs, a record that has been broken by April of this year. So let me ask you, Mr. Van Valkenburgh, a study came out earlier this year that said that 80 percent of ICOs in 2017 were scams. SEC Chairman Jay Clayton has suggested the right approach to uncovering the scams and protecting investors is to regulate ICOs as security offerings, and I just want to ask if you agree with that approach. I know we are over time, but if I could just permit the witness to answer.

Mr. VAN VALKENBURGH. I do agree with that approach. As I said, the majority of ICOs have either been unregistered securities issuance or scams, as Chairman Clayton has said. The SEC has made very careful and deliberate policy here. I think they have done an excellent job. They released a report helping people understand these things. They created a website helping them understand them in a visual, physical way. And they have brought targeted enforcement actions that I think have started to chill these markets and make them more rational.

That said, I think you can do a token sale and comply with securities laws, as you should, and we are seeing the emergence of companies doing that, selling only to accredited investors, or—and I think this will happen in the near future—even doing public registration and offering tokens to shareholders.

Senator WARREN. But what I hear you saying at its core is that an unregulated market puts consumers at risk, and what is critical is to get the right regulations in place.

Mr. VAN VALKENBURGH. Often our current regulations. Securities laws worked well for the last 100 years, or almost, and I think they will continue to.

Senator WARREN. All right. Thank you.

Senator BROWN. Senator Van Hollen.

Senator VAN HOLLEN. Thank you. Thank you both for being here.

Dr. Roubini, you mentioned your support for digital payment systems innovation, and FinTech clearly has reduced inefficiencies in the payment system. It has not yet succeeded in getting the Fed, though, to move to a real-time payment system, something I have been pushing hard for, because the current system where it takes time still to clear checks has really been hurting a lot of lower-income people who are living paycheck to paycheck. I was pleased to see the Fed recently announce that it is going to try and accelerate this effort.

Do you have an opinion on using innovation to get to real-time payment system as the Fed is moving toward, I hope?

Mr. ROUBINI. Yes, I am all in favor of it, and technology can be used to achieve that particular result. In principle, you know, the banks have access to the balance sheet of the Fed, but you could have a system where every corporation or individual has access to that balance sheet. You do not need to have a blockchain for that. You have it on one ledger. It is secured by the Fed. And if you do that, however, you have consequences, because right now the deposits in the banking system are essentially forms of money that are sent to the payment system. If you go to a central bank in digital currency and you have everybody accessing that one, then there will be massive disintermediation of private deposits, and then the banks have to fund themselves in a different way.

So there is talk about going in that direction, of opening up the balance sheet of the central bank to everybody, but it has important consequences for the financial system.

The point, however, is that you can do all these things, but you don't need blockchain. Or if you want a system——

Senator VAN HOLLEN. I am not disagreeing——

Mr. ROUBINI.——it is not going to be a public one where a bunch of miners in China are going to verify the transactions of our financial system. That does not make any sense.

Senator VAN HOLLEN. I am not disagreeing with you, Dr. Roubini. I have just been pushing—I have been disappointed the Fed has not moved more quickly to implement a real-time payment system, and I think that fact is a drag on a lot of consumers.

While I have got you here, though, I do want to ask you a question of where you see the economy going, because you are one of the people who predicted the 2008 financial crash. You not only predicted it, but you predicted the mechanics and the economic and financial forces behind it. And you have written about your concern about the economy around 2020, a concern I share, and I just want to note your article of September 11th, "Is the next financial crisis already brewing?" where you talk about the fact that the stimulus, which was the sort of tax cuts, which added $1.8 trillion to our debt, was ill-timed, that it will create a drag on the economy in a number of years, and that you foresee difficult economic times ahead.

Given that you predicted the 2008 financial crash, I thought I would take the time to get your opinion on where we are headed right now.

Mr. ROUBINI. Well, in brief, I would say this year growth is going to be because of the stimulus close to 3 percent. It is going to be less than 3 percent next year. My concerns are about 2020, one, because we will have a fiscal cliff; second, because the Fed, rightly, with an overheating economy has to gradually increase interest rates. Short rates are going to go higher, long rates are going to go higher. The dollar is going to strengthen. Credit spreads are going to widen. That tightening of financial condition is going to slow economic growth.

I worried about protectionism and trade wars slowing down economic growth, and I also worried about other stagflationary policies like restricting migration, restricting capital inflows and outflows and FDI, restricting investment in the environment and not having an infrastructure plan, reducing growth and increasing inflation.

We also know that asset prices are faulty, and if there is a shock to growth, there could be a significant correction. So those combination of factors may lead to a stall of economic growth by 2020.

Senator VAN HOLLEN. Well, you summarized it very well, and my question to you, if you could just take a moment and talk about something many of us have said is likely to happen, which is when you have an economy that was already on a rapidly rising trajectory, and you add to that a huge amount of debt, how that creates a fiscal drag and crowds out private investment down the road and actually slows down the economy after the overheating period is over. Can you just talk about that for a second?

Mr. ROUBINI. Yeah, briefly. It is the first time we have a $2 trillion fiscal stimulus in peacetime without a recession. That leads to higher short-term and long-term interest rates. It leads to overheating and forces the Fed to hike more, soon, and faster. It leads to a stronger dollar. And it also leads to a larger current account and trade deficit. If the savings of the Government reduce, our trade deficit is 2 percent of GDP, it is going to go toward 3 percent and, therefore, the protectionist pressure may increase over time. So it is an ill-advised fiscal stimulus.

Senator VAN HOLLEN. Thank you. I appreciate it.

Chairman CRAPO. Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you. Thank you, gentlemen, for being here.

I would like to go back to Senator Jones' conversation with you when it comes to identifying sex trafficking, drug trafficking, money laundering, and I just want some clarification. Mr. Van Valkenburgh, does Bitcoin or any similar platform have a protocol in place to detect when its cryptocurrency is being used by individuals to facilitate sex trafficking, drug trafficking, or money laundering? Is there a protocol in place?

Mr. VAN VALKENBURGH. So Bitcoin is a peer-to-peer network of persons running software around the world, and that software is developed itself by people around the world. It is a voluntary system, if you will, so there is no corporate form to set and guarantee policies across all users.

That said, there are several intermediaries who are building their businesses on top of Bitcoin, just as you saw several companies build their businesses on top of the shared and open internet back in the 1990s. And those businesses, especially those that are based and regulated here in the United States, do have those policies for identifying and policing illicit use of the network, and they do file suspicious activity reports, and they do register with FinCEN, which is our financial surveillance authority.

Senator CORTEZ MASTO. So it is going to be incumbent upon those businesses, basically what you are saying, working with law enforcement to identify when this technology they are utilizing is engaging in illicit activity?

Mr. VAN VALKENBURGH. That is right, Senator.

Senator CORTEZ MASTO. Would you agree with that, Dr. Roubini?

Mr. ROUBINI. Well, I do agree that in the United States there are rules about KYC/AML that are being implemented. But suppose you are involved in human trafficking and you are setting up a Bitcoin account somewhere in a jurisdiction or offshore financial center where these KYC/AML rules are not being followed, and then you are doing those activities and using these foreign accounts, and it is anonymous, it is very hard to crack down on them, and, therefore, you are not under the scope of U.S. legislation, and you have created an asset class that allows this massive level of anonymity. So unless you have a global agreement first at the G–20, but then covers the rest of the world that makes sure that those rules are applied by everybody else, you have created a massive loophole that allows terrorists, traffickers, tax evaders, or criminals to do it more easily than in the past. That is a major risk.

Senator CORTEZ MASTO. Thank you, Dr. Roubini.

Yes, please?

Mr. VAN VALKENBURGH. First of all, I would just be interested in how you can use something that is not money to evade taxes, but that is a separate issue. I will say that with respect to international exchanges, I absolutely agree that we should have a unified global approach to ensure that there is KYC. But I will disagree that if you are just transacting on the blockchain, even using the account that you originally created in an overseas authority that did not collect information, that it is, as Dr. Roubini says, anonymous, it is not anonymous at all. And I have spoken with several law enforcement officials and investigators who, as I said, enjoy doing their blockchain investigations because they can track every transaction with perfect fidelity on the block chain, very different than the international correspondent banking system where you have shell accounts and bad records and records all over at different institutions.

A good example of this is BTC-e, which was an exchange based somewhere in Eastern Europe that was being used to launder money. FinCEN, in combination with the DOJ, brought an investigation. They looked at the blockchain. They found transactions all from that exchange heading to a wallet, all the fee transactions. They said, OK, this was the person running this illicit enterprise, and they ultimately were able to identify him based on that information, and they arrested him when he was, I think, on holiday in Greece. His name is Alexander Vinnik.

Senator CORTEZ MASTO. I appreciate that. And the reason why I asked the question, because I think it is important as we go down this path and we are looking at the use of this new technology that we continue to study it. That is why Senator Toomey and I introduced the Fight Illicit Networks and Detect Trafficking Act. The bill would require the GAO to study how virtual currencies like Bitcoin and other online marketplaces use, buy, sell, facilitate the financing of goods and how it is affiliated, if any, with illicit activity.

So let me move on because I am running out of time. I am curious, Dr. Roubini, I also sit on Energy and Natural Resources. We have had this conversation about the use of blockchain technology in the energy sector and how it is going to be a game changer for the energy sector. Have you studied the use of this blockchain technology in any other sectors other than the financial sector? Have you looked at it and its use in the energy sector at all?

Mr. ROUBINI. Well, I have not looked at it in the energy sector, but, of course, people talk about using it in the case of commodities. My point is that even if you use what is called "blockchain technologies" to do transactions, say, in energy and commodities, you are never going to use a public, trustless, permission-less, peer-to-peer distributed system. It does not make any sense. So if you are using it private, permission with trusted authorities, that is not a blockchain. It is a system where you have trusted authority with verified transactions that say these sets of transactions are OK. So there are sophisticated versions of databases, but they are not blockchain. They are not based on cryptographic consent mechanisms that let a bunch of people in China or Russia authenticate your transactions. No commodity exchange, no commodity business is going to let that happen. It is going to be private and permissioned. So it is not a blockchain. I think it is a misnomer calling these things "blockchains."

Senator CORTEZ MASTO. Thank you.

Chairman CRAPO. [Presiding.] Thank you. And that does conclude our questioning. I apologize to the witnesses. I had to step out. I am also a member of a couple other committees, and one of them was having a markup that I had to vote at. So I apologize that I was absent for part of your answers.

For Senators wishing to submit questions for the record, those questions are due in 1 week, on Thursday, October 18. And to our witnesses, we ask that you respond to those questions as quickly as you can. And, again, thank you for being here today. Obviously, there is a significant difference of opinions on these issues, but I do not think there is any disagreement that these are critical issues that we need to face and deal with.

With that, thank you for being here today, and the hearing is adjourned.

[Whereupon, at 11:03 a.m., the hearing was adjourned.]

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

PREPARED STATEMENT OF CHAIRMAN MIKE CRAPO

Today, the Committee will continue its exploration of the opportunities and challenges surrounding the cryptocurrency and blockchain ecosystem.

Prior to the introduction of Bitcoin and underlying blockchain ledger in 2009, there was no similar solution to the double-spend problem—where the same digital currency could be spent more than once—which did not require a third-party intermediary.

While Bitcoin, the first decentralized cryptocurrency, has been around for nearly a decade now, cryptocurrencies have gained particular attention in the past 2 years, due in part to their meteoric rise and subsequent fall in value last year.

Advancements since Bitcoin's creation have expanded blockchain's uses and given way to things like "Initial Coin Offerings," a method of crowdfunding that has become popular in the cryptocurrency community.

While the technologies underpinning cryptocurrencies have the ability to transform the composition of, and ability to access, capital and the financial system, much of the recent news about cryptocurrencies has been negative, focusing on enforcement actions, hacks on international exchanges, and concerns raised by various regulators and market participants.

To that end, in February of this year, the Committee held a hearing with the SEC and CFTC to examine their oversight roles of cryptocurrency-related products and activities under their respective jurisdictions.

Since that hearing, the agencies have made strides to provide further clarification on their thinking surrounding cryptocurrency-related issues.

But, some regulatory and oversight questions still remain.

The regulatory questions, price volatility and reports of things like pump-and-dump schemes have raised a lot of questions surrounding the cryptocurrency and blockchain ecosystem that need to be better understood.

Blockchain networks have the potential to improve processes for things like smart contracts, payments and settlement, identity management and even things yet undiscovered.

In order to move forward in a productive way and give these innovations the room to flourish and develop in a safe and sound way, we need to sort through the static and better understand what exactly are the opportunities and challenges facing this ecosystem.

For example, the Committee would benefit to hear about: the use of cryptocurrencies and derivative products as a store of value or medium of exchange or payment; the current and potential applications of blockchain technology; and the regulatory issues surrounding the various facets of the ecosystem and how they can be improved.

PREPARED STATEMENT OF SENATOR SHERROD BROWN

Thank you, Chairman Crapo, for holding this hearing. And thank you to Mr. Van Valkenburgh and Dr. Roubini for your testimony.

Today's hearing happens to fall just shy of the tenth anniversary of Bitcoin and the blockchain being introduced to the world—October 31, 2008. Back then we were in the midst of a global financial crisis, and you can't blame some Americans for hoping that an alternative banking system could be created that would be superior to the one in shambles at that time.

Bitcoin, and other cryptocurrencies like it, promised to make payments faster, easier and cheaper, and to eliminate our reliance on risky financial institutions whose failures harmed workers and families during the crisis.

Unfortunately, the last 10 years have shown that misconduct, fraudulent investment schemes, and cybersecurity threats aren't unique to the traditional financial system. When a cryptocurrency goes bust or a poorly supervised exchange fails, it's often hardworking Americans left holding the bag.

We want to see innovations in the financial system, innovations that help Americans keep more of their money by avoiding fees or that make it easier to borrow for a small business startup.

But so far, despite all the energy and investment dedicated to finding a use for the blockchain, there are few real-world applications and an alarming number of scams.

Cryptocurrency prices have swung wildly over the last year. Inexperienced investors who were hoping to get in on the next big financial innovation have seen the value of these investments fall by more than 75 percent from their peak.

Though they have raised billions of dollars from investors, few if any Initial Coin Offerings have registered with the SEC. Chair Clayton told this Committee in a February hearing, "Every ICO I've seen is a security."

And last month, the New York Attorney General released a report on several cryptocurrency trading platforms that pointed to evidence of widespread manipulation and identified several exchanges that don't follow "anti-money laundering" or "know your customer" requirements.

With a decade of experience, much of the irrational exuberance around cryptocurrencies and blockchain technology has subsided, and we have an opportunity to set more realistic expectations for how these innovations might be used to promote a fairer and more competitive economy.

I hope this technology will prove useful, particularly in helping people who are unbanked or underserved by the traditional financial system. And I understand why individuals might be interested in it. But at this point, it is easier to see the malign impacts on society as a whole than the constructive ones.

I look forward to the witnesses' testimony.

PREPARED STATEMENT OF NOURIEL ROUBINI, PH.D.

PROFESSOR OF ECONOMICS, STERN SCHOOL OF BUSINESS, NEW YORK UNIVERSITY

OCTOBER 11, 2018

Chairman Crapo, Ranking Member Brown and Members of the Committee, thank you for the opportunity to testify today on the topic of the Cryptocurrency and Blockchain Ecosystem.

My name is Nouriel Roubini and I am a Professor of Economics at the Stern School of Business at New York University. I am an expert of the global economy, international financial markets, asset and credit bubbles and their bust, and the related financial crises. I was one of the few economists warning about and predicting in advance the Global Financial Crisis of 2007–2009 and I am one of the leading global scholars on the topic of bubbles and financial crises. My most recent book "Crisis Economics: A Crash Course in the Future of Finance" is a seminal treatise on the topic of asset bubbles and financial crises. I have written dozens of papers and other contributions on the topic of bubbles and their bust and the causes and consequences of financial crises.

Crypto Bubble (2017) and Crypto Apocalypse and Bust (2018)

It is clear by now that Bitcoin and other cryptocurrencies represent the mother of all bubbles, which explains why literally every human being I met between Thanksgiving and Christmas of 2017 asked me first if they should buy them. Especially folks with zero financial literacy—individuals who could not tell the difference between stocks and bonds—went into a literal manic frenzy of Bitcoin and Crypto buying. Scammers, swindlers, criminals, charlatans, insider whales and carnival barkers (all conflicted insiders) tapped into clueless retail investors' FOMO ("fear of missing out"), and took them for a ride selling them and dumping on them scammy crappy assets at the peak that then went into a bust and crash—in a matter of months—like you have not seen in any history of financial bubbles.

A chart of Bitcoin prices compared to other famous historical bubbles and scams—like Tulip-mania, the Mississippi Bubble, the South Sea Bubble—shows that the price increase of Bitcoin and other crypto junk-coins was 2X or 3X bigger than previous bubbles and the ensuing collapse and bust as fast and furious and deeper. Bitcoin rapidly exploded in 2017 from $1k to $10k and then peaked almost at $20k in December 2017 only to collapse to below $6k (down 70 percent from that peak) in a matter of 4 months and it has been close to $6k since then. And a 70 percent capital loss was a "good" deal compared to thousands of alt-coins (otherwise better known as "sh*tcoins") that have lost on average 95 percent of their value since the peak. Actually calling this useless vaporware garbage a sh*tcoin is a grave insult to manure that is a most useful, precious and productive good as a fertilizer in agriculture.[1]

Now that the crypto bloodbath is in full view the new refuge of the crypto scoundrels is "blockchain," the technology underlying crypto that is now alleged to be the cure of all global problems, including poverty, famines and even diseases. But as discussed in detail below blockchain is the most over-hyped—and least useful—

[1] My apologies to the Members of the Senate Banking Committee for using the scatological term "sh*tcoin" but the term is standard in the crypto jargon and there are more than 500,000 references to it in a Google search of this technical term. See: *https://www.google.com/search?q=shitcoin&oq=shitco&aqs=chrome.0.0j69i57j0l4.3571j0j8&sourceid=chrome&ie=UTF-8.*

technology in human history: in practice it is nothing better than a glorified spreadsheet or database.

The entire cryptocurrency land has now gone into a crypto-apocalypse as the mother and father of all bubbles has now gone bust. Since the peak of the bubble late last year Bitcoin has fallen by about 70 percent in value (depending on the week). And that is generous. Other leading cryptocurrencies such as Ether, EOS, Litecoin, XRP have fallen by over 80 percent (or more depending on the week). While thousands of other cryptocurrencies—literally scam-coins and scam-tokens—have fallen in value between 90 percent and 99 percent. No wonder as a recent study showed that 81 percent of all ICOs were scams in the first place, 11 percent of them are dead or failing while only 8 percent of them are traded in exchanges. And out of this 8 percent the top 10 coins traded—after Bitcoin—have lost between 83 percent and 95 percent of their value since peak with an average loss of over 90 percent. This is a true Crypt-Apocalypse. No wonder that a recent study this week argued and conclude that the crypto industry is on the "brink of an implosion."[2]

No asset class in human history has ever experienced such a rapid boom and total utter bust and implosion that includes thousands of different crypto-assets.

Crypto is not money, not scalable

To be a currency, Bitcoin—or any cryptocurrencies—should be a serviceable unit of account, means of payments, and a stable store of value. It is none of those things. No one prices anything in Bitcoin. Few retailers accept it. And it is a poor store of value, because its price can fluctuate by 20–30 percent in a single day. And since its price has been so unstable or volatile almost no merchant will ever use it as a means of payment: the profit margin of any merchant can be wiped out in a matter of minutes—if he or she accepts Bitcoin or any other cryptocurrency—by the change in the dollar price of a cryptocurrency. Proper means of payments need to have stable purchasing power; otherwise no one will ever use them.

As is typical of a financial bubble, investors were buying cryptocurrencies not to use in transactions, but because they expected them to increase in value. Indeed, if someone actually wanted to use Bitcoin, they would have a hard time doing so. It is so energy-intensive (and thus environmentally toxic) to produce, and carries such high transaction costs, that even Bitcoin conferences do not accept it as a valid form of payment (*https://slate.com/technology/2018/01/the-most-important-blockchain-conference-of-the-year-wont-take-bitcoin-for-last-minute-sales.html*). Paying $55 dollars of transaction costs to buy a $2 coffee cup is obviously never going to lead Bitcoin to become a transaction currency.

Until now, Bitcoin's only real use has been to facilitate illegal activities such as drug transactions, tax evasion, avoidance of capital controls, or money laundering. Not surprisingly, G20 member states are now working together to regulate cryptocurrencies and eliminate the anonymity they supposedly afford, by requiring that all income- or capital-gains-generating transactions be reported. Even the U.S. Treasury Secretary Steve Mnuchin has publicly stated that we cannot allow cryptocurrencies to become the next Swiss bank account.

Since the invention of money thousands of years ago, there has never been a monetary system with hundreds of different currencies operating alongside one another. The entire point of money is that it allows parties to transact without having to barter. But for money to have value, and to generate economies of scale, only so many currencies can operate at the same time.

In the United States, the reason we do not use euros or yen in addition to dollars is obvious: doing so would be pointless, and it would make the economy far less efficient. The idea that hundreds of cryptocurrencies could viably operate together not only contradicts the very concept of money with a single numeraire that can be used for the price discovery of the relative price of thousands of good; it is utterly idiotic as the use of multiple numeraires is like the stone age of barter before money was created.

Supply of crypto is massive. Bitcoin is deflationary

But so, too, is the idea that even a single cryptocurrency could substitute for fiat money. Cryptocurrencies have no intrinsic value, whereas fiat currencies certainly do, because they can be used to pay taxes. Fiat currencies are legal tender and can be used and are used to buy any good or service; and they can be used to pay for tax liabilities. They are also protected from value debasement by central banks committed to price stability; and if a fiat currency loses credibility, as in some weak

[2] *https://www.newsbtc.com/2018/10/09/juniper-research-the-crypto-industry-is-on-the-brink-of-an-implosion/.*

monetary systems with high inflation, it will be swapped out for more stable foreign fiat currencies—like the dollar or the euro—or real assets such as real estate, equities and possibly gold. Fiat money also is not created out of thin air: these liabilities of a central bank such as the Fed are backed by the Fed assets: their holdings of short term and longer term Treasury securities (that have near AAA sovereign credit status in the United States) and holding of foreign reserves including gold and other stable foreign currencies. The usual crypto critique of fiat currencies that can be debased via inflation is nonsense: for the last 30 years commitment to inflation targeting in advanced economies and most emerging markets has led to price stability (the 2 percent inflation target of most central banks) and for the last decade the biggest problem of central banks has been that achieving the inflation target of 2 percent after the GFC has become extremely difficult as, in spite of unconventional monetary policies, the inflation rate has systematically undershot its 2 percent target.

Instead 99.9 percent all cryptocurrencies instead have no backing whatsoever of any sort and have no intrinsic value of any sort; and even the so-called "stable coins" have only partial backing at best with true U.S. dollars reserves or, like Tether, most likely no backing at all as there has never been a proper audit of their accounts.

As it happens, Bitcoin's supposed advantage is also its Achilles's heel, because even if it actually did have a steady-state supply of 21 million units, that would disqualify it as a viable currency. Unless the supply of a currency tracks potential nominal GDP, prices will undergo deflation.

That means if a steady-state supply of Bitcoin really did gradually replace a fiat currency, the price index of all goods and services would continuously fall. By extension, any nominal debt contract denominated in Bitcoin would rise in real value over time, leading to the kind of debt deflation that economist Irving Fisher believed precipitated the Great Depression. At the same time, nominal wages in Bitcoin would increase forever in real terms, regardless of productivity growth, adding further to the likelihood of an economic disaster.

Worse, cryptocurrencies in general are based on a false premise. According to its promoters, Bitcoin has a steady-state supply of 21 million units, so it cannot be debased like fiat currencies. But that claim is clearly fraudulent, considering that it has already forked off into several branches and spin-offs: Bitcoin Cash and Bitcoin Gold. Ditto for the various forks and spin-off of Ether from the Ethereum cartel. It took a century for Coca Cola to create the new Coke and call the old one Coke Classic. But it took 3 years to Ethereum to dump the first ETH into Ethereum Classic and create and brand new spin-off, ETH.

Moreover, hundreds of other cryptocurrencies are invented every day, alongside scams known as "Initial coin offerings," which are mostly designed to skirt securities laws. And their supply is created and debased every day by pure fiat and in the most arbitrary way. So cryptocurrencies are creating crypto money supply and debasing it at a much faster pace than any major central bank ever has. No wonder that the average cryptocurrency has lost 95 percent of its value in a matter of a year.

At least in the case of Bitcoin the increase in supply is controlled by a rigorous mining process and the supply is capped—at the limit—to 21 million bitcoins. Instead, most other alt-coins starting with the leading ETH, have an arbitrary supply that was created via pre-mining and pre-sale; and the change of supply of that and thousands of other cryptocurrencies is now subject to arbitrary decision of self-appointed "central bankers."

And the biggest scam of all is the case of "stable coins"—starting with Tether—that claimed to be pegged one-to-one to the U.S. dollar but are not fully collateralized by an equal backing of true U.S. dollars. Bitfinex—behind the scammy Tether—has persistently refused to be properly audited and its creation of fiat Tether has been systematically used to prop up manipulate upward the price of Bitcoin and other cryptocurrencies according to a recent academic paper.[3]

Financial crises occurred well before fiat currencies and central banking; and are now less virulent thanks to central banks and fiat money.

Another totally false argument is that asset and credit bubbles are caused by central banks and the existence of fiat currencies. Any student of financial crises knows that asset and credit bubbles were widespread before fiat currencies and central banks were created; see for example Tulipmania, the Mississippi Bubble and the South Sea Bubble. These bubbles and their busts were frequent, virulent and had

[3] *https://www.bloomberg.com/news/articles/2018-06-13/professor-who-rang-vix-alarm-says-tether-used-to-boost-bitcoin.*

massive economic and financial costs including severe recessions, deflations, defaults and financial crisis.

Central banks—instead—were initially created not to provide goods price stability but rather to provide financial stability and avoid the destructive bank, sovereign and currency runs that do occur when a bubble goes bust. Indeed, the Fed was created in 1913 when the last of many bubbles gone bust that had caused massive bank runs led to the realization that an institution that could provide with lender of last resort to the financial system was needed. That and the creation of deposit insurance after the Great Depression is the reason why bank runs are so rare. And the purpose of fiat currencies whose supply is regulated by credible and independent central bank is to reduce the frequency, virulence and severity of economic recessions, deflations and asset and credit bubbles gone bust. And indeed the economic and financial history of the United States and other countries shows that severe economic recessions, depressions, deflations and financial crises are less frequent and less costly after the creation of fiat currencies and central banks.

Crypto-currencies instead have not and will never have the tools to pursue economic and financial stability. The few like Bitcoin whose supply is truly constrained by an arbitrary mathematical rule will never be able to stabilize recessions, deflations and financial crises; they will rather lead to permanent and pernicious deflation. While the rest—99 percent—have an arbitrary supply generation mechanism that is worse than any fiat currency and, at the same time, will never be able to provide either economic or price or financial stability. They will rather be tools of massive financial instability if their use were to become widespread.

The real revolution in financial services is FinTech and it has nothing to do with Blockchain or Crypto

The financial-services industry has been undergoing a revolution. But the driving force is not overhyped blockchain (*https://medium.com/@pavelkravchenko/decline-of-blockchain-hype-and-rise-of-a-common-sense-8de5789a794d*) applications such as Bitcoin. It is a revolution built on artificial intelligence, big data, and the Internet of Things.

Already, thousands of real businesses are using these technologies to disrupt every aspect of financial intermediation. Dozens of online-payment services—PayPal, Venmo, Square and so forth—have hundreds of millions of daily users in the United States. Billions more use similar low cost, efficient digital payment systems all over the world: AliPay and WeChat Pay in China; UPI-based systems in India; M–Pesa in Kenya and Africa. And financial institutions are making precise lending decisions in seconds rather than weeks, thanks to a wealth of online data on individuals and firms. With time, such data-driven improvements in credit allocation could even eliminate cyclical credit-driven booms and busts.

Similarly, insurance underwriting, claims assessment and management, and fraud monitoring have all become faster and more precise. And actively managed portfolios are increasingly being replaced by passive robo-advisers, which can perform just as well or better than conflicted, high-fee financial advisers.

Now, compare this real and ongoing FinTech revolution that has nothing to do with blockchain or cryptocurrencies with the record of blockchain, which has existed for almost a decade, and still has only one failing and imploding application: cryptocurrencies.

Buterin's inconsistent trinity: crypto is not scalable, is not decentralized, is not secure

There is a deeper fundamental flaw and inconsistency in the crypto/blockchain space. As Vitalik Buterin correctly wrote a while ago there is a fundamental "inconsistent trinity" in blockchain: you cannot have at the same time scalability, decentralization and security.

Bitcoin, for example, is partially decentralized—even if its mining is now massively centralized—but it is not scalable given its proof of work (PoW) authentication mechanism—that allows only for 5 to 7 transactions a second. And it is secure—so far—but at the cost of no scalability. And since its mining is now massively centralized—as an oligopoly of miners now control its mining—its security is at risk.

Supporters of crypto have been promising forever—Buterin spoke of Proof of Stake (PoS) in 2013—systems that are vastly scalable. But leaving aside that PoS is not live yet and Ethereum is still based on PoW, the reality is that once Proof of Stake is properly launched it will be massively centralized and thus not secure. The whole logic of PoS is to give greater voting power to those who have a stake in a coin—those who own it the most and mine it the most. But that leads to a massive centralization problem. Even Bitcoin that is based on PoW has seen a massive centralization and concentration of mining power in a small oligopolistic group. This problem of concentration of mining power among an oligopoly becomes much worse with PoS as those with greater initial stake—and Ethereum is massively concentrated in ownership of ETH—will get a greater stake over time. So the problems of oligopolistic cartelization of mining power that is already very serious in PoW will become exponentially worse in PoS.

More generally, while cryptography scientists are busy inventing every day another "consensus" mechanism and there are dozens of new ones after PoW and PoS and their variant the reality is that—given Buterin's inconsistent trinity it will never be possible to create a consensus mechanism that is scalable while also being decentralized and secure.

One solution to the problem of scalability is to use many alt-coins rather than increasing the block size of each blockchain; but that solution is highly inefficient and is not secure. A second solution is to increase the block size; but then nodes running on a smaller computer or laptop would drop out of the system as they will not be able to store every transaction or state. So you would end up relying on a small number of super-computers for running the blockchain; so you end up with an oligopoly with market power, concentration and lack of security. A third solution is where most of the crypto industry is trying to go, *i.e.,* merge mining and variant of proof of stake. In this system there are many chains but all such chains share the same mining power or stake. But this approach increases the computational and storage demands on each miner by a massive factor that most miners will not be able to support. So this solution is a backdoor way of increasing the size of the blocks. Thus, it leads to only very few powerful miners to participate into this proof of stake, *i.e.,* participating in merge-mining each chain. So it leads again to centralization, oligopolies of mining and thus lack of security.

Whichever way you try to slice it blockchain leads to centralization and lack of security. And this fundamental problem when you try scalability will never be resolved. Thus, no decentralized blockchain will ever be able to achieve scalability that is critical to make it useful for large scale financial or any other type of transactions. Indeed, even those blockchains that do not have any scalability, like Bitcoin and those based on PoW, have massive mining concentration problems. The nature of mining implies that any form of mining has economies of scale that require massive scale—think of the massive energy hogging mining factories of crypto-land—and lead to massive oligopolistic concentration of power and lack of security.

With the centralization of power comes a serious problem of lack of security, starting with 51 percent attacks. Supporters of crypto argue that it would not be in the interest of an oligopoly of miners to start a 51 percent as it would destroy their source of income/fees. But leaving aside that such an attack would allow them to steal the underlying assets—worth is some cases dozens of billions of dollars as in the case of BTC. The main problem is any oligopolistic cartel will end up behaving like an oligopoly: using its market power to jack up prices, fees for transactions and increase its profit margins. Indeed, as concentration of mining has increased over the last year transaction costs of crypto—as measured by miners' fees divided by number of transactions—have skyrocketed.

No security in cryptocurrencies

So even PoW that is not scalable leads to concentration/centralization and thus lack of security. PoS and other authentication mechanisms that are scalable are much worse: bigger concentrated oligopolistic cartels and thus lack of security.

Also 51 percent attacks are not a theoretic possibility that is impossible in practice. Dozens of successful 51 percent attacks have occurred recently. In smaller coins with a small market capitalization you don't even need a 51 percent hash power to mount a successful 51 percent attack. And since market cap is low a few hundreds of thousands of dollars—or at best a couple of millions—are sufficient to mount a successful 51 percent attack whose gain is a 10 to 20X multiple of the cost of the attack. No wonder that dozens of successful 51 percent attack have occurred recently against smaller cryptocurrencies.

Fundamental flaws of lack of security in crypto land go well beyond the fact that mining is highly concentrated in oligopolies in shady and nontransparent and unsecure jurisdictions—China, Russia, Belarus, Georgia, *etc.* It also goes beyond the possibility and reality of massive and regular 51 percent attacks.

There is a deeper and more fundamentals set of security flaws in crypto land. Conventional payment systems based on fiat currencies, central banks and private banks are scalable and secure but centralized; so they resolve Buterin's inconsistent trinity principle by giving up decentralization and relying on trusted permissioned authorities to resolve the "double spend" problem.

Instead, blockchains and cryptocurrencies not only are not scalable and are massively centralized; they are also massively not secure.

When I use traditional financial systems based on fiat currencies there are many levels and layers of security. First I rely on institutions with a reputation and credibility built over time; there is also deposit insurance that guarantees the value of my deposits; there is the lender of last resort role of central bank to avoid runs on solvent but illiquid banks; sometimes even there is even the bailout of systemically important too-big-to-fail (TBTF) institutions with provisos to control this TBTF moral hazard. More importantly, a depositor or credit card holder is made whole with little effort when fraudulent transaction occur and someone tries to steal your money or make a fraudulent charge on your credit card. Society pays a small fee—in a number of ways—to ensure such safety but depositors and credit card holders are happy to pay such a modest fee in exchange for transaction security. So while many breaches of security may occur—as there are main weak points in the system—the system is secure and individual users of the system are also secure.

In crypto land instead there are none of these institutions that provide security: no deposit insurance, no lender of last resort backstop, no insurance of hacked and stolen funds. And the breaches of security are massive and escalating. It is now clear that while Bitcoin has not been hacked yet the centralized exchanges that hold the cryptocurrencies of millions of depositors can be and have been hacked on a regular scale. And once your crypto assets are stolen they vanish in the vast anonymous void of crypto and cannot be found and retrieved any more. The vast hacking of centralized exchanges has led to the developments of dozens of decentralized exchanges (DEX) but 99 percent of all trading is on centralized exchanges and some security flaws of DEX imply that even the so called “secure” DEX are not secure at all. Once a hacker steals your private key—whether it is stored on an online wallet, laptop, phone, computer or tablet or centralized exchange your crypto wealth is stolen and gone forever.

Given these massive security problems of crypto the solutions to these severe security problems are all variants of going back to the stone age: do not put your long private key—that no human can memorize ever—on any digital device but rather write it down on a piece of paper and hide it in a hole where hopefully no one will find it or no insect or rat will destroy it. Or spend a fortune to put your crypto assets into “cold storage”, *i.e.,* a digital storage that is disconnected from anything online. The latter is the stone age equivalent of hiding your wealth into deep caves that cannot be found by anyone. But leaving aside the cost of such stone age security solutions the implication becomes that your crypto wealth—hidden in deep cold storage—cannot be easily traded or used for transactions of any sort. This is the contemporary equivalent of mining gold deep from the ground and then hiding it in the form of gold ingots back deep in the ground.

Even such security solutions are not safe: criminals who know that access to your private key is access to your entire crypto wealth forever are now specializing into gunpoint robberies of crypto investors and whales (also known as “crypto robberies”). At gunpoint you are forced to provide your private key and then your wealth is gone for good. No wonder that crypto conferences have entire sessions devoted to secure your insecure crypto assets.

Traditional banking systems have found secure solutions to such criminal security problems: even if a robber forces you at gunpoint to reveal the pin of your ATM card the amount of cash that can be withdrawn is limited to a small amount; similarly wire transfer of a significant size are subject to various forms of identity verification. o there is no way that your entire wealth can be stolen with a click as it happens daily in crypto land. While crypto relies on stone age technologies and cannot even resolve such security problems.

Decentralization is a self-serving ideology

Blockchain’s ideology is politically born out of the same mentality as libertarian right wing conspiracies or extreme left anarchism: all governments, central banks, moneys, institutions, banks, corporations, entities with reputation and credibility build over centuries are evil centralized concentrations of power that literally need to be destroyed.

So the utopian crypto future will be one of libertarian decentralization of all economic activity, transactions and human interactions. Everything will end up on a public decentralized distributed permission-less, trustless ledger; or better millions of ledgers on computers that are now already consuming more energy than Canada to verify and confirm transactions without the use of evil centralized institutions. This extreme right wing ideology of crypto has been studied in detail in the academic book by David Golumbia "The Politics of Bitcoin: Software As Right Wing Extremism."[4]

But the reality is just the opposite: a bunch of self-serving greedy white men—very few women or minorities are allowed in the blockchain space—have pretended to create billions of wealth out of nowhere while pretending to care about billions of poor and unbanked human around the world. It is a total pretense as crypto-land is the most centralized scam in human history where greed for Lambos and ostentatious consumption is greater than any Gordon Gecko ever.

There are hundreds of stories of greedy crypto-criminals raising billions of dollars with scammy white papers that are nothing but vaporware and then literally stealing these billions to buy Lambos, expensive cars, villas in the Caribbean and the French Riviera. These large scale criminals stealing dozens of billions make the small and petty Wolf of New York robbing small investors in criminal penny stock manipulation schemes looks an amateur.

But the most shameful of such near-criminals is a crypto guru—that was formerly investigated for pedophilia and who has put his home and operation—together with a group of crypto scammers—in Puerto Rico after a devastating hurricane that killed thousands and nearly destroyed the island.

Under the high-flatulent pretense of wanting to help the millions who lost homes and their livelihood to the hurricane by using "blockchain" and new crappy cryptocurrencies these literal blood-suckers live in super-luxury mega mansions in the island and use the island's tax laws to enrich themselves and avoid paying their Federal taxes. They are emblematic of a widespread crypto culture that shamelessly pretends to care about the billions of poor and unbanked just to enrich itself. At least the Wolf of New York had no pretense of wanting save the world, end global poverty and the tragic misery of a Puerto Rico devastated by a hurricane.

Decentralization is a myth: massive centralization and concentration of oligopolistic power and cartels among miners, exchanges, developers, wealth holders.

The reality is one of a massive centralization of power among miners, exchanges, developers and wealth holders, the total opposite of the lie of a decentralized system.

First, miners are massively centralized as the top four among them control three quarters of mining and behave like any oligopolist: jacking up transaction costs to increase their fat profit margins. And when it comes to security most of these miners are in nontransparent and authoritarian countries such as Russia and China. So we are supposed not to trust central banks or banks when it comes to financial transactions but rather a bunch of shady anonymous concentrated oligopolists in jurisdictions where there is little rule of law?

A recent study by a scholar at Princeton University is aptly titled "The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin."[5] In summary the conclusions of this paper are as follows: "As Bitcoin's popularity has grown over the decade since its creation, it has become an increasingly attractive target for adversaries of all kinds. One of the most powerful potential adversaries is the country of China, which has expressed adversarial positions regarding the cryptocurrency and demonstrated powerful capabilities to influence it. In this paper, we explore how China threatens the security, stability, and viability of Bitcoin through its dominant position in the Bitcoin ecosystem, political and economic control over domestic activity, and control over its domestic internet infrastructure. We explore the relationship between China and Bitcoin, document China's motivation to undermine Bitcoin, and present a case study to demonstrate the strong influence that China has over Bitcoin. Finally, we systematize the class of attacks that China can deploy against Bitcoin to better understand the threat China poses. We conclude that China has mature capabilities and strong motives for performing a variety of attacks against Bitcoin."

Everything that this study argues about the nefarious impact of China on Bitcoin can be said and applied to any other cryptocurrency and to the role of Russia in the crypto eco-system.

Second, all trading is centralized as 99 percent of all trading occurs on centralized exchanges while hundreds of decentralized exchanges have no trading, no liquidity are collapsing. And centralized exchanges are being hacked daily as there is not security in keeping crypto assets in a wallet; and once hacked your wealth is gone forever.

[4] *https://www.upress.umn.edu/book-division/books/the-politics-of-bitcoin.*

[5] *https://arxiv.org/pdf/1810.02466.pdf.*

Third, development is centralized as Vitalik Buterin—creator of Ethereum—is named as "benevolent dictator for life". And there is nothing immutable in the "code is law" motto as the developers are police, prosecutors and judges: when something goes wrong in one of their buggy "smart" pseudo-contracts[6] and massive hacking occurs, they simply change the code[7] and "fork" a failing coin into another one by arbitrary fiat,[8] revealing the entire "trustless" enterprise to have been untrustworthy from the start.

"Smart Contracts" are neither smart nor contracts. As a recent study has shown "smart contracts on Ethereum are worse than even nonfinancial commercial code; as of May 2016, Ethereum contracts averaged 100 obvious bugs (so obvious a machine could spot them) per 1000 lines of code. (For comparison, Microsoft code averages 15 bugs per 1000 lines, NASA code around 0 per 500,000 lines.)"[9]

Fourth, wealth in crypto-land is more concentrated than in North Korea where the inequality Gini coefficient is 0.86 (it is 0.41 in the quite unequal United States): the Gini coefficient for Bitcoin is an astonishing 0.88 (*https://www.businessinsider.com/bitcoin-inequality-2014-1*).

Quite a feat to create an asset class where inequality is greater than that of Kim Jong-un land.

So decentralization is just a total myth invented by a bunch of whales whose wealth is fake; now that the retail suckers who bought at the peak have literally lost their shirts these crypto "whales" are fake billionaires as liquefying their wealth would crash the price of the "asset" to zero.

Crypto is not the internet nor will it ever be

Blockchain's boosters would argue that its early days resemble the early days of the internet, before it had commercial applications. But that comparison is simply false. Whereas the internet quickly gave rise to email, the World Wide Web, and millions of viable commercial ventures used by billions of people in less than a decade, cryptocurrencies such as Bitcoin do not even fulfill their own stated purpose (*https://www.project-syndicate.org/commentary/why-bitcoin-is-a-bubble-by-nouriel-roubini-2018-01?barrier=accesspaylog.)*

The comparison with the early days of the internet is nonsense as even the early internet in the early 1990s saw a rapid boom of applications and explosion of user adoption: email became widespread and thousands of useful website used by millions of people for useful purpose sprang overnight. The boom in web sites creation was so vast, rapid and massive that early on directories of such web site—such as the start of Yahoo—and search engines became necessary to navigate the richness of information of the World Wide Web (WWW).

The WWW went live in 1991 and by 2000—nine years later—it already had 738 million users; and by 2015 the number of users was 3.5 billion.

Crypto has been around for over a decade now and in 2018 the number of crypto wallets was only 22 million and out of this figure the number of active Bitcoin users is only between 2.9 and 5.9 million and falling. And the number of crypto transactions has collapsed by at least 75 percent between 2017 and 2018.

Successful new technologies have a few key features: exponential increase of the number of users, exponential increase of the number of transaction, sharp and persistent fall of transaction costs. That is the history of the internet—almost one billion users in a decade since start and billions of billions of transactions in the first decade—and is also the history of financial markets where trading activity—say in equity markets—includes an exponential increase in users, exponential and permanent increase in number of transactions and a sharp fall in transaction costs (as measured by falling bid-ask spreads and by the collapse of brokers' fee for equity transactions).

Crypto land is just the opposite: the number of users in a decade is still barely 22 million globally and, after the bust of crypto in 2018, the active users are a fraction of that number; the number of transactions on crypto exchanges in 2018 has collapsed and is down between 75 percent and 80 percent; same for the size of transaction values given the collapse of crypto asset prices; and transaction costs are surging through the roof rather than falling as measured by the total value of miners revenue as a share of the number of transactions. And after over a decade crypto land has not a single killer app.

[6] *https://davidgerard.co.uk/blockchain/ethereum-smart-contracts-in-practice/.*

[7] *https://www.coindesk.com/the-dao-bitcoin-development/.*

[8] *https://www.cbc.ca/news/technology/ethereum-hack-blockchain-fork-bitcoin-1.3719009.*

[9] *https://davidgerard.co.uk/blockchain/ethereum-smart-contracts-in-practice/.*

So crypto and blockchain are not like the early years of the internet that was booming in every dimension in its first decade; it is instead literally collapsing and imploding in every possible dimension. It is a failing set of technologies.

ICOs are not compliant securities when they aren't outright scams

Initial coin offerings have become the most common way to finance cryptocurrency ventures, of which there are now nearly 1,600 and rising (*https://coinmarketcap.com/all/views/all/*) . In exchange for your dollars, pounds, euros, or other currency, an ICO issues digital "tokens," or "coins," that may or may not be used to purchase some specified good or service in the future.

Thus it is little wonder that, according to the ICO advisory firm Satis Group, 81 percent of ICOs are scams (*https://medium.com/@sherwin.dowlat/cryptoasset-market-update-b678aeda4c5e*) created by con artists, charlatans, and swindlers looking to take your money and run. It is also little wonder that only 8 percent of cryptocurrencies end up being traded on an exchange, meaning that 92 percent of them failed. It would appear that ICOs serve little purpose other than to skirt securities laws that exist to protect investors from being cheated.

If you invest in a conventional (noncrypto) business, you are afforded a variety of legal rights—to dividends if you are a shareholder, to interest if you are a lender, and to a share of the enterprise's assets should it default or become insolvent. Such rights are enforceable because securities and their issuers must be registered with the State.

Moreover, in legitimate investment transactions, issuers are required to disclose accurate financial information, business plans, and potential risks. There are restrictions limiting the sale of certain kinds of high-risk securities to qualified investors only. And there are anti-money-laundering (AML) and know-your-customer (KYC) regulations to prevent tax evasion, concealment of ill-gotten gains, and other criminal activities such as the financing of terrorism.

In the Wild West of ICOs, most cryptocurrencies are issued in breach of these laws and regulations, under the pretense that they are not securities at all but rather "security tokens."[10] Hence, most ICOs deny investors any legal rights whatsoever. They are generally accompanied by vaporous "white papers" instead of concrete business plans. Their issuers are often anonymous and untraceable. And they skirt all AML and KYC regulations, leaving the door open to any criminal investor.

Jay Clayton, the chairman of U.S. Securities and Exchange Commission, recently made it clear that he regards all cryptocurrencies as securities, with the exception of the first mover, Bitcoin, which he considers a commodity (*https://finance.yahoo.com/news/sec-ico-tokens-regulated-securities-205650102.html*). The implication is that even Ethereum and Ripple—the second- and third-largest crypto-assets—are currently operating as unregistered securities.[11] Gary Gensler, a former chairman of the Commodities and Futures Trading Commission who now teaches a course on blockchain (*https://www.project-syndicate.org/commentary/blockchain-technology-limited-applications-by-nouriel-roubini-and-preston-byrne-2018-03?barrier=accesspaylog*) (the technology underlying cryptocurrencies) at MIT, has also suggested as much (*https://www.bloomberg.com/news/articles/2018-04-23/ether-ripple-may-be-securities-former-cftc-head-gensler-says*).

And legal scholars such as Preston Byrne have not only confirmed that they Ether was created makes it a clear security.[12] They have also shown that the creation of Ethereum may have been a criminal insider con job where a small group of whale—starting with the billionaires who created this scheme—pretended to make a market-based "pre-sale" of Ether but they instead sold to themselves—most likely at bargain basement prices—a great fraction of the ETH created in the pre-sale. And so far regulators have done nothing to investigate, let alone, prosecute such a cartelized scam.

Tokenization: cartels aimed to gouge consumers. No numeraire and return to barter

So hundreds of ICOs that have raised billions of dollars from investors in recent years have been technically illegal as they are noncompliant securities hiding under the label of "security tokens". Even worse, the business model behind most of the remaining ones—the so-called "utility tokens"—is simply to fleece customers, as Izabella Kaminska of the Financial Times and Martin Walker of the Center for Evidence-Based Management recently demonstrated in a report (*http://*

[10] We will discuss below the other scam of so-called "utility token."

[11] A legal scholar such as Preston Byrne has shown that Ripple Labs has created XRP; see *https://prestonbyrne.com/2018/09/20/for-the-last-time-ripple-created-xrp/*.

[12] *https://prestonbyrne.com/2018/04/23/on-ethereum-security/*.

data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/digital-currencies/written/82032.html) for the U.K. House of Commons Treasury Committee.

In normal business transactions, customers can buy goods and service with conventional currencies. But in an ICO, customers must convert that currency by buying into a limited pool of tokens in order to make a purchase. No legitimate business that is trying to maximize profits would require its customers to jump through such hoops of first buying an "utility token" before being able to transact goods or services.

In fact, the only reason to restrict a purchase to token-holders is to create an illegal cartel of service providers who are safe from price competition and in a position to gouge their customers. Consider Dentacoin, a ridiculous cryptocurrency that can be spent only on dental services (and which almost no dentist actually accepts). It would be hard to come up with a better illustration of why business cartels are illegal in all civilized countries.

Of course, the crypto-cartels would counter that customers who incur the cost of buying a token will benefit if that token appreciates in value. But this makes no sense. If the price of the token rises above the market value of the good or service being provided, then no one would buy the token. The only plausible reason for forcing the use of a token, then, is to hike prices or bilk investors.

Beyond facilitating illegal activity, crypto-tokens obfuscate the price-discovery benefits that come when a single currency operates as a unit of account. In a crypto-utopia, every single good and service would have its own distinct token, and average consumers would have no way to judge the relative prices of different—or even similar—goods and services. Nor would they have any real certainty about a token's purchasing power, given the volatility of crypto-token prices.

Imagine living in a country where instead of simply using the national currency, you had to rely on 200 other world currencies to purchase different goods and services. There would be widespread price confusion, and you would have to eat the cost of converting one volatile currency into another every time you wanted to buy anything.

The fact that everyone within a given country or jurisdiction uses the same currency is precisely what gives money its value. Money is a public good that allows individuals to enter into free exchange without having to resort to the kind of imprecise, inefficient bartering on which traditional societies depended.

That is precisely where the ICO charlatans would effectively take us—not to the futuristic world of "The Jetsons," but to the modern Stone Age world—that is worse than "The Flintstones"—who at least used clam shells as their money and understood the importance of a single numeraire—where all transactions occur through the barter of different tokens or goods. It is time to recognize their utopian rhetoric for what it is: self-serving nonsense meant to separate credulous investors from their hard-earned savings.

Massive manipulation: pump-and-dump, spoofing, wash trading, front running, exchanges conflicts of interest, Tether scam

There is now massive evidence—from serious press investigations and academic studies—that the entire crypto-land is subject to massive, systematic and widespread price manipulation of every sort known in the annals of criminal manipulation: pump-and-dump schemes, wash trading, spoofing, front-running, serious conflicts of interest between exchanges and their customers, vast insider trading, creation of pseudo stable coins that are rather fiat cryptocurrencies that are used only to prop up Bitcoin and other cryptocurrencies. While price manipulation does occur in a variety of financial markets, there are strict laws against it and it is subject to draconian criminal prosecution; thus, it is the exception rather than the rule. While criminal price manipulation and insider trading is systemic in crypto land. For example, various investigations by the Wall Street Journal have shown that hundreds of criminal "pump-and-dump" chat rooms exist on the Telegram chap app that are aimed only at systematically manipulating the price of hundreds of cryptocurrencies.[13]

In 2018 cryptocurrency values fell by 90 percent on average from their December peak. They would have collapsed much more had a vast scheme to prop up their price via outright manipulation not been rapidly implemented (*https://coinreport.net/teetering-tether/*). But, like in the case of the sub-prime bubble, most U.S. regulators are still asleep at the wheel while having started investigations months ago.

[13] *https://www.wsj.com/graphics/cryptocurrency-schemes-generate-big-coin/*.

The mother of all manipulations in the crypto land is related to Tether and Bitfinex—a shady crypto exchange—that is its backer. Bitfinex—behind the scammy Tether—has persistently refused to be properly audited and has hopped on four continents changing every season the shady bank that provides it banking service linked to fiat dollars. And the supply of Tether is increased randomly—by hundreds of millions of chunks at a time via pure fiat—as a way to manipulate and prop up the value of Bitcoin and the entire related cryptocurrency system. Tether has already created by fiat billions of dollars of a "stable coin" that has never been audited. The creation of fiat Tether has been systematically used to prop up manipulate upward the price of Bitcoin and other cryptocurrencies according to a recent academic paper by a leading scholar at the University of Texas. Without such outright criminal manipulation the price of Bitcoin would now be about 80 percent lower than its current value, *i.e.,* about $1200 rather than the current $6500.[14]

No killer app in crypto/blockchain after a decade: only ponzi schemes

Even supporters of crypto and blockchain do admit that there no killer app in crypto or blockchain even after a decade of developments and attempts. And as shown above the comparison with the early days of the internet is utter nonsense as the internet had massive adoption and many early killer apps or websites.

The only think that Crypto/Blockchain is DAPPS or Distributed Apps. But recent studies show that 75 percent of the highly illiquid and bared used DAPPS are Krypto-Kitties, Pyramid and Ponzi schemes and Casino games. And the Ethereum community is doing nothing—literally nothing to stop or block such Ponzi games as it parasitically financially profits from them. The remaining 25 percent of DAPPS are decentralized exchanges that no one uses as 99 percent of all crypto trading occurs on centralized exchanges. So pretty much most DAPPS are scams or useless gimmick and their transaction volumes are close to zero. Pretty much no adoption of anything. So the comparison with early days of the internet is nonsense.

The energy consumption of crypto is an environmental disaster

The environmental costs of the energy use of Bitcoin and other cryptocurrencies is so vast that has been correctly and repeatedly compared to an environmental disaster. No need to repeat how such energy mis-use and waste is massive—larger than the energy use per year of a mid-sized advanced economy. Such an environmental disaster has shamed even supporters of crypto who have become defensive given the embarrassing evidence of such energy costs and pollution.

But now zealot supporters of crypto are pretending that this environmental disaster can be minimized or resolved soon. Since using millions of computers to do useless cryptographic games to secure the verification of crypto transactions is a useless waste of energy—as the same transactions could be reported at near zero energy costs on an single Excel spreadsheet—crypto zealots argue that such costs could be massively reduced if crypto moves from energy-hogging PoW to less energy-wasteful Proof of Stake. But as we discussed above in detail, scalability of crypto transactions via PoS will be massively concentrated in dangerous oligopolies—even more so than PoW—and therefore such centralization of mining power will lead to most severe problems of security. So, there is no free lunch here. Either crypto keeps on using energy-hogging and environmental-disaster PoW or it will become an insecure, centralized, and dangerous system.

The other argument made by crypto zealots is that other financial activities—such as gold mining or running the traditional financial system—hog a lot of energy. Those apologies are utter nonsense. The mining of gold or the provision of financial services produces value added and output to the economy that is 1000X than the pseudo value added of crypto mining. And financial services provide payment and other services to billions of people daily in hundreds of billions of daily transactions. So of course their use of energy will be larger than crypto. Crypto is used by 22 million folks globally—less than 5 million active ones today—and its entire market cap is 200 billion—not the 300 trillion of global financial and real assets—and is producing value added that is a few billions a year—new crypto mining. But its energy use cost is already about $5 billion a year. So comparing the energy use of useless, inefficient and tiny crypto to the services of financial institutions serving daily billions of people is utter nonsense of comparing apples and oranges or, better, crypto parasites with useful financial services (payments, credit, insurance, asset management, capital market services) used by billions. That is why a recent scholar

[14] *https://www.bloomberg.com/news/articles/2018-06-13/professor-who-rang-vix-alarm-says-tether-used-to-boost-bitcoin.*

has defined Bitcoin as being "as efficient as a lame hippopotamus with an hangover."[15]

Blockchain is most overhyped technology ever, no better than a glorified spreadsheet or database

And why is blockchain no better than an Excel spreadsheet or database?

There is no institution under the sun—bank, corporation, nonprofit, Government, charity—who would put on public, decentralized, peer-to-peer permission-less, trustlees, distributed ledgers its balance sheet, P&L, transactions, trades, interactions with clients and suppliers. Why should all this information—mostly proprietary and highly valuable—be on a public ledger and authenticated by some random, not transparent and shady group of "miners"? No reason and thus there is NO institution whatsoever using a public, permission-less distributed technology.

The only applications of blockchain—so called "enterprise DLT"—have in reality absolutely nothing to do with blockchain. They are private not public, they are centralized not decentralized, they are not distributed as they are on a few controlled ledgers not millions of public ones, they are permissioned with very few legitimate individuals authorized to add and change the ledgers rather than being permissionless, they are based on trusted authorities that have reputation and credibility build over time rather than being trustless, they are not peer-to-peer as a centralized and permissioned intermediary is in charge of authentication. In other term they are called blockchains but they are not blockchains as they have nothing to do with a public distributed ledger technology.

So all so called "decentralized" blockchains end up being centralized private permissioned databases, *i.e.,* effectively no improvement over using an Excel spreadsheet rather than hogging more energy than most large-sized economies to put private information on millions of computers all over the world.

And no wonder as no person or firm or institution in authority in the private or public sector would ever allow all of its transactions to be verified by an oligopoly of shady nontransparent agents in autocratic countries where all power is centralized. So it is no surprise that any institution under the sun after experimenting with a pilot "blockchain" dumps it into the garbage bin or turns it into a private permissioned database that is no "blockchain" in any dimension but its misleading name.

Also as for the underlying pseudo-blockchain technology, there are still massive obstacles standing in its way. Chief among them is that it lacks the kind of basic common and universal protocols that made the internet universally accessible (TCP–IP, HTML, and so forth): there are 1000s different "blockchain" incompatible with each other and totally lacking the critical "inter-operability" that the internet had from the beginning. More fundamentally, its promise of decentralized transactions with no intermediary authority amounts to an untested, Utopian pipedream (*https://www.ft.com/content/b5b1a5f2-5030-11e7-bfb8-997009366969*). No wonder blockchain is ranked close to the peak of the hype cycle of technologies with inflated expectations (*https://www.project-syndicate.org/commentary/why-bitcoin-is-a-bubble-by-nouriel-roubini-2018-01?barrier=accesspaylog*).

So blockchain is one of the most overhyped technologies ever (*https://www.project-syndicate.org/commentary/why-bitcoin-is-a-bubble-by-nouriel-roubini-2018-01?barrier=accesspaylog*). Blockchains are less efficient than existing databases. When someone says they are running something "on a blockchain," what they usually mean is that they are running one instance of a software application that is replicated across many other devices.

If it is truly distributed the required storage space and computational power is substantially greater, and the latency higher, than in the case of a centralized application. Blockchains that will incorporate "proof-of-stake" or "zero-knowledge" technologies will require that all transactions be verified cryptographically, which slows them down. Blockchains that use "proof-of-work," as many popular cryptocurrencies do, raise yet another problem: they require a huge amount of raw energy to secure them and are not scalable. This explains why Bitcoin "mining" operations in Iceland are on track to consume more energy this year than all Icelandic households combined (*http://www.bbc.co.uk/news/technology-43030677*).

Blockchains can make sense in cases where the speed/verifiability tradeoff is actually worth it, but this is rarely how the technology is marketed. Blockchain investment propositions routinely make wild promises to overthrow entire industries, such as cloud computing, without acknowledging the technology's obvious limitations.

Consider the many schemes that rest on the claim that blockchains are a distributed, universal "world computer." That claim assumes that banks, which already

[15] *https://prestonbyrne.com/2018/10/05/bitcoin__hippo/*.

use efficient systems to process millions of transactions per day, have reason to migrate to a markedly slower and less efficient single cryptocurrency. This contradicts everything we know about the financial industry's use of software. Financial institutions, particularly those engaged in algorithmic trading, need fast and efficient transaction processing. For their purposes, a single globally distributed blockchain such as Ethereum would never be useful and they will never use it.

Another false assumption is that blockchain represents something akin to a new universal protocol, like TCP–IP or HTML were for the internet. Such claims imply that this or that blockchain—among thousands that are incompatible with each other—will serve as the basis for most of the world's transactions and communications in the future. Again, this makes little sense when one considers how blockchains actually work. For one thing, blockchains themselves rely on protocols like TCP–IP, so it isn't clear how they would ever serve as a replacement.

Furthermore, unlike base-level protocols, blockchains are "stateful," meaning they store every valid communication that has ever been sent to them. As a result, well-designed blockchains need to consider the limitations of their users' hardware and guard against spamming. This explains why Bitcoin Core, the Bitcoin software client, processes only 5–7 transactions per second, compared to Visa, which reliably processes 25,000 transactions per second (*https://www.project-syndicate.org/commentary/blockchain-technology-limited-applications-by-nouriel-roubini-and-preston-byrne-2018-03?barrier=accesspaylog#*).

Just as we cannot record all of the world's transactions in a single centralized database, nor shall we do so in a single distributed database. Indeed, the problem of "blockchain scaling" is still more or less unsolved, and is likely to remain so forever.

Although we can be fairly sure that blockchain will not unseat TCP–IP, a particular blockchain could eventually set a standard for specific private permissioned, not general and public, applications, just as Enterprise Linux and Windows did for PC operating systems. But betting on a particular "coin," as many investors currently are, is not the same thing as betting on adoption of a larger "protocol" that does not require the use of any coin. Given what we know about how open-source software is used, there is little reason to think that the value to enterprises of specific blockchain applications will capitalize directly into any coin.

A third false claim concerns the "trustless" utopia that blockchain will supposedly create by eliminating the need for financial or other reliable intermediaries. This is absurd for a simple reason: every financial contract in existence today can either be modified or deliberately breached by the participating parties. Automating away these possibilities with rigid "trustless" terms is commercially nonviable, not least because it would require all financial agreements to be cash collateralized at 100 percent, which is insane from a cost-of-capital perspective (*https://prestonbyrne.com/2017/12/10/stablecoins-are-doomed-to-fail/*).

Moreover, it turns out that many likely appropriate applications of blockchain in finance—such as in securitization or supply chain monitoring—will require permissioned centralized intermediaries after all, because there will inevitably be circumstances where unforeseen contingencies arise, demanding the exercise of discretion. The most important thing blockchain will do in such a situation is ensure that all parties to a transaction are in agreement with one another about its status and their obligations before a trusted and permissioned central authority verifies the transaction.

It is high time to end the hype. Bitcoin is a slow, energy-inefficient dinosaur that will never be able to process transactions as quickly or inexpensively as an Excel spreadsheet. Ethereum's plans for an insecure proof-of-stake authentication system will render it vulnerable to manipulation by influential insiders. And Ripple's technology for cross-border interbank financial transfers is already left in the dust by SWIFT, a nonblockchain consortium that all of the world's major financial institutions already use (*https://www.swift.com/our-solutions/swift-gpi#*). And the technology behind Ripple is different from its coin XRP: some may use the technology/protocol but no one will use the underlying coin whose value has collapsed. Ditto for Ether versus Ethereum. Similarly, centralized e-payment systems with almost no transaction costs—Faster Payments, AliPay, WeChat Pay, Venmo, Paypal, Square—are already being used by billions of people around the world who are doing billions of low cost/fee secure transactions.

Ultimately, private permissioned blockchain's uses will be limited to specific, narrow well-defined, and complex applications that require transparency and tamper-resistance more than they require speed. So they are not truly a "blockchain".

A case in point, among hundreds of other cases, is the recent announcement of the IBM food "blockchain" going live with a major supermarket giant being on board with this project. Leave aside that the success of such a project—as any other Enterprise DLT one—is more than sketchy as there is no general accepted protocol to make this system inter-operable among thousands of users and customers. The key issue is—as the IBM spokesman quoted in the article say—that this system "obviously requires the growers, the suppliers, and the retailers all to be part of the solution, sending in information in a trusted and permissioned fashion and we link it all together."[16] So this alleged blockchain system is trusted not trustless, permissioned not permission-less and managed and linked strictly by IBM, not a distributed peer-to-peer consensus mechanism managed by millions of anonymous computers. Therefore, this project has nothing to do with blockchain, as defined in standard terms. It is a traditional database with the usual key elements of a private, permissioned databased managed by centralized and trusted authorities. And the same exact model is the base of any other Enterprise DLT: none of them have anything substantial to do with blockchain even if they use this faddy and catchy label.

Enterprise DLT/Blockchain: All hype and no reality

This is also the reason why corporate blockchains or Enterprise DLT are another fad this is now fading and imploding, as a recent Bloomberg analysis revealed.[17] Most companies will halt their blockchain or DLT tests this year; and in 90 percent of the cases "the experiments will never become part of a company's operations." An analyst from Gartner—the leading tech research firm—concluded: "The disconnect between the hype and the reality is significant—I've never seen anything like it. "In terms of actual production use, it's very rare."

And the interest in corporate blockchain is collapsing: "Only 1 percent of chief information officers said they had any kind of blockchain adoption in their organizations, and only 8 percent said they were in short-term planning or active experimentation with the technology, according to a Gartner study. Nearly 80 percent of CIOs said they had no interest in the technology."

Crypto is corrupt eco-system full of charlatans, con-men, self-interested insiders and scammers. But I have NO conflict of interest

Crypto-land is an eco-system of con artists, self-serving peddlers, scammers, carnival barkers, charlatans, and outright criminals. While every successful technological revolution includes some bubbles and some scammers, most of the real ones—like the internet—create real goods and services that billions of folks use around the world even after the initial frothiness and bubble has burst. And the criminal and scamming element in real technological revolutions is the exception, not the systemic rule that it is in crypto land. Scams in cryptocurrencies were so widespread and systemic that the SEC had to create a fake website that parodies the scammy ICO to warns investors of the plethora of scams and criminal enterprises that infest and dominate crypto land.[18]

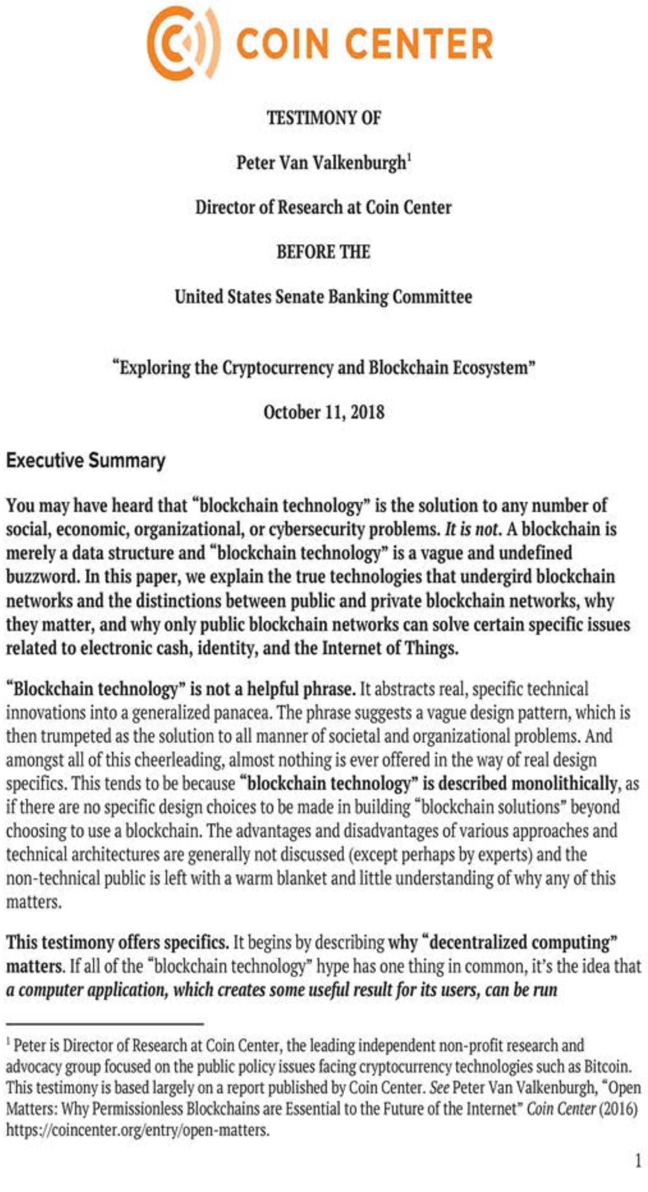
This scammy eco-system is consistent with the idiotic crypto jargon: HODLers are suckers who have hold on their collapsing cryptocurrencies even after they lost 90 percent of their value; Lambos refer to the crypto obsession with stealing investors' money to buy luxury energy hogging cars; Whales are large early crypto billionaires who are stuck with their fake wealth after the suckers of retails investors—who bought into the FOMO of the peak 2017 bubbles—lost 90 percent of their investments; those suckers are also called BagHolders. The entire crypto jargon is not of a new industry developing a creative disruptive technology but that of an industry of con artists, criminals, scammers and carnival barkers.

Unlike all self-interested crypto insiders and scammers who talk and spin their book 24/7 and use a media/press eco-system of pseudo-journalists to spin their endless fake news I have zero position and financial interest in this entire space. I have zero long or short position in any coin or cryptocurrency and any blockchain business venture. And even my support of nonblockchain FinTech is not driven from any direct or indirect financial interest; I have zero exposure to FinTech ventures. Bitcoin or any crypto-asset could go "To The Moon" or crash to zero and I would not make a penny either way. The only thing that is at stake is my personal, intellectual and academic reputation.

[16] *https://www.coindesk.com/ibm-food-supplychain-blockchain-carrefour-live-production/.*

[17] *https://www.bloomberg.com/news/articles/2018-07-31/blockchain-once-seen-as-a-corporate-cure-all-suffers-slowdown.*

[18] *https://www.marketwatch.com/story/the-sec-created-a-mock-ico-website-to-show-just-how-easy-it-is-for-investors-to-get-fleeced-2018-05-16.*



TESTIMONY OF

Peter Van Valkenburgh[1]

Director of Research at Coin Center

BEFORE THE

United States Senate Banking Committee

"Exploring the Cryptocurrency and Blockchain Ecosystem"

October 11, 2018

Executive Summary

You may have heard that "blockchain technology" is the solution to any number of social, economic, organizational, or cybersecurity problems. *It is not*. A blockchain is merely a data structure and "blockchain technology" is a vague and undefined buzzword. In this paper, we explain the true technologies that undergird blockchain networks and the distinctions between public and private blockchain networks, why they matter, and why only public blockchain networks can solve certain specific issues related to electronic cash, identity, and the Internet of Things.

"Blockchain technology" is not a helpful phrase. It abstracts real, specific technical innovations into a generalized panacea. The phrase suggests a vague design pattern, which is then trumpeted as the solution to all manner of societal and organizational problems. And amongst all of this cheerleading, almost nothing is ever offered in the way of real design specifics. This tends to be because **"blockchain technology" is described monolithically**, as if there are no specific design choices to be made in building "blockchain solutions" beyond choosing to use a blockchain. The advantages and disadvantages of various approaches and technical architectures are generally not discussed (except perhaps by experts) and the non-technical public is left with a warm blanket and little understanding of why any of this matters.

This testimony offers specifics. It begins by describing **why "decentralized computing" matters**. If all of the "blockchain technology" hype has one thing in common, it's the idea that ***a computer application, which creates some useful result for its users, can be run***

[1] Peter is Director of Research at Coin Center, the leading independent non-profit research and advocacy group focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. This testimony is based largely on a report published by Coin Center. *See* Peter Van Valkenburgh, "Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet" *Coin Center* (2016) https://coincenter.org/entry/open-matters.

simultaneously on many computers around the world rather than on just one central server, and that the network of computers can work together to run the application in a way that avoids trusting the honesty or integrity of any one computer or its administrators. To describe this idea we prefer the term "decentralized computing" to "blockchain technology," because it is more descriptive and it is also a broader category.

This testimony demystifies the actual technologies behind "blockchain technology" and explains these *several* technologies in a way that even non-technical readers will understand. This testimony creates a typology of "blockchain technologies" and it will suggest that only certain *types* of "blockchain technology" can be real solutions to certain major social and organizational challenges.

For starters, rather than talking about "blockchain technology" in the abstract, we discuss the real technical innovations that underlie Bitcoin, the actual functioning technology that has spurred all the blockchain hype. There are really **three core innovations** that underlie Bitcoin: **peer-to-peer networking**, **blockchains**, and **consensus mechanisms**. Of these, peer-to-peer networking is generally nothing new, and blockchains are merely novel ways of storing and validating data. ***Consensus mechanisms, however, are the truly disruptive, interesting, and critical component of the design.*** **When it comes to capabilities, risks, and disruptive potential, however, not all consensus mechanisms are created equal.** The critical nature of consensus mechanisms in these new blockchain-powered decentralized computing systems, and the variability in types of consensus mechanism design are why the bulk of this testimony focuses on explaining consensus mechanisms to non-technical audiences.

In general, **by consensus we simply mean the process by which a number of computers come to agree on some shared set of data and continually record valid changes to that data.** So the blockchain might be the form that the data take, *e.g.* a hashed list of valid transactions in bitcoin, but it is the consensus mechanism that generates that blockchain, validates the data, and continually keeps the data updated and reconciled between all of the computers in the system.

This brings us to the question of "publicness" in the consensus mechanism. Who is allowed to read the data over which the network is forming consensus, and possibly more important, who is allowed to participate in the process that ultimately results in new data being added? Are some consensus mechanisms more open to free participation than others? **In a public consensus mechanism anyone with a computer and an internet connection should be eligible to play a role in writing consensus data; in a private consensus mechanism only those who have been identified by a centralized authority and given an authorization credential are allowed to participate.**

The operation of various consensus mechanisms is described in the full testimony. Public consensus mechanisms include **proof-of-work** based mechanisms, as found in Bitcoin and most cryptocurrencies, as well as **proof-of-stake** mechanisms and **social consensus** mechanisms. Private consensus mechanisms generally follow what we call a **consortium consensus** model, wherein only identified and credentialed consortium members share the privilege of writing consensus data.

From an **innovation policy** perspective, public consensus mechanisms are superior to their private counterparts because they create purpose-agnostic platforms atop which anyone with a connected computer can build, test, and run user-facing decentralized applications. In this sense, **networks powered by public consensus mechanisms mirror the early Internet, and may one day become as indispensable as the Internet in facilitating free speech, competition, and innovation in computing services.**

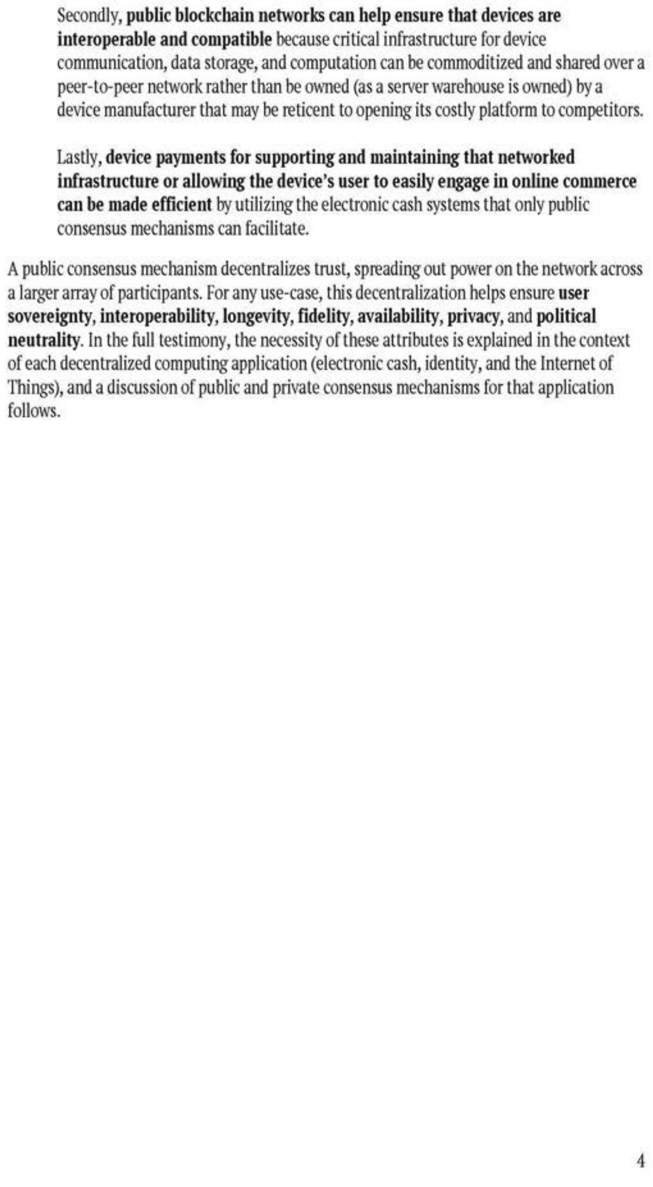
Apart from publicness, we also discuss the nature of **trust** and **privacy** in each of the several consensus mechanisms. Public consensus mechanisms demand that users place trust in unknown third parties who are economically motivated to behave honestly because they have **skin in the game** and face **competitive pressures**. Private consensus mechanisms demand that users place trust in the identifying authority who provisions consortium members with credentials, and the honesty and cybersecurity practices of the members themselves. Public consensus mechanisms trade **transparency** for **privacy** but new technologies such as **zero-knowledge proofs** and **homomorphic encryption** may enable public networks to have superior privacy and verifiability as compared with private networks that rely only on **perimeter security** to maintain privacy.

Finally, we explain why public consensus mechanisms, specifically, are critical for three particular decentralized computing applications: **electronic cash, identity, and the Internet of Things**.

- **Electronic Cash.** Truly electronic ***cash*** (*i.e.* fungible bearer assets, the use of which resembles that of paper notes) offers **efficiencies that existing electronic money transmission systems cannot**. There are hidden costs to legacy systems: chargebacks, and transactions forgone because fees are greater than the value being sent or because participants cannot obtain a banking relationship. Fundamentally, from a user's perspective, a private-blockchain money transmission technology doesn't "just work" from the get-go. I cannot send or receive money until I open an account and establish a legal relationship with a company. This may be a tolerable inconvenience, but it is not a system that works like cash, which can be accepted in the hand without any prior arrangements in place. **Only public consensus mechanisms, by fully automating the creation and maintenance of a ledger according to pre-established rules and economic incentives, can offer electronic transactions that are as good as cash.**

- **Identity. The Internet lacks a native identity layer.** This shortcoming is the reason why Internet users must rely on a tapestry of weak passwords, secret questions, and knowledge of mothers' maiden names to verify their identity to various web service providers. The need for a better solution is widely recognized, and **by creating a shared and unowned platform for recording identity data, public blockchains may provide the answer.**

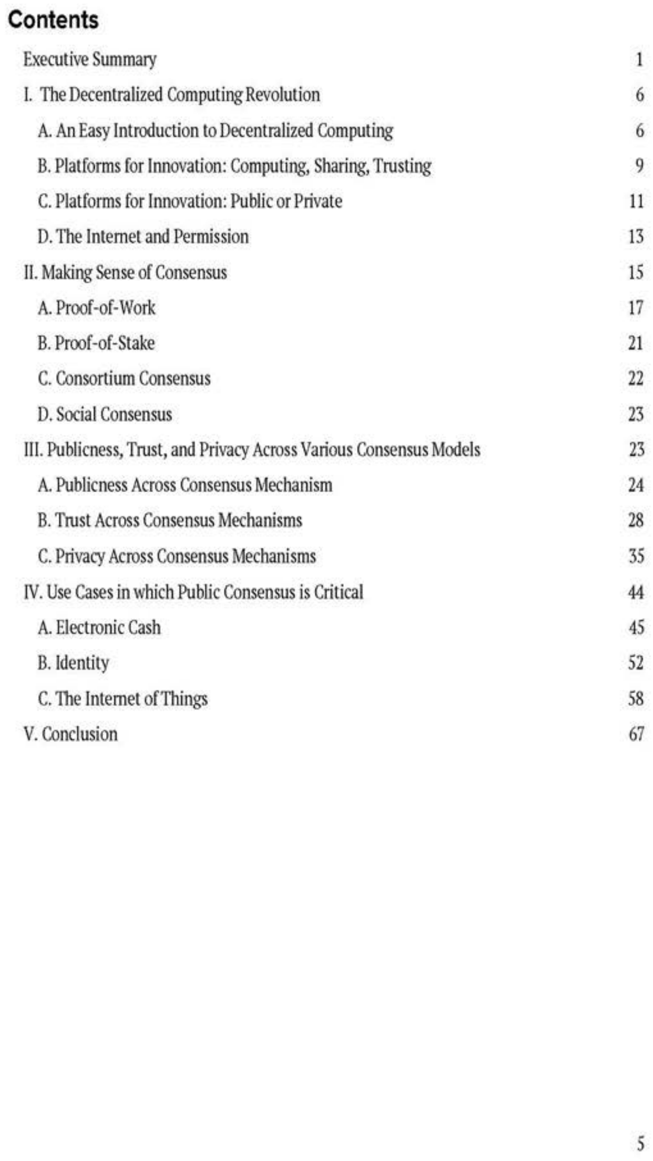
- **The Internet of Things.** Firstly, public blockchain networks allow for a truly decentralized data structure for device identity (I am a bulb in this home's kitchen) and user access authorization (the user with address 0xE1A... is the only person who can turn me on and off). The redundant and decentralized nature of data on these networks can ensure that these systems have true longevity, and that **a manufacturer's decision to end support for a product will not destroy the user's ability to securely access the product's features**.



Secondly, **public blockchain networks can help ensure that devices are interoperable and compatible** because critical infrastructure for device communication, data storage, and computation can be commoditized and shared over a peer-to-peer network rather than be owned (as a server warehouse is owned) by a device manufacturer that may be reticent to opening its costly platform to competitors.

Lastly, **device payments for supporting and maintaining that networked infrastructure or allowing the device's user to easily engage in online commerce can be made efficient** by utilizing the electronic cash systems that only public consensus mechanisms can facilitate.

A public consensus mechanism decentralizes trust, spreading out power on the network across a larger array of participants. For any use-case, this decentralization helps ensure **user sovereignty**, **interoperability**, **longevity**, **fidelity**, **availability**, **privacy**, and **political neutrality**. In the full testimony, the necessity of these attributes is explained in the context of each decentralized computing application (electronic cash, identity, and the Internet of Things), and a discussion of public and private consensus mechanisms for that application follows.



Contents

I. The Decentralized Computing Revolution

If all of the "blockchain technology" hype has one thing in common, it's the idea that a computer application, which creates some useful result for its users, can be run simultaneously on many computers around the world rather than on just one central server, and that the network of computers can work together to run the application in a way that avoids trusting the honesty or integrity of any one computer or its administrators. To describe this idea, we prefer the term "decentralized computing" to "blockchain technology," because it is more descriptive and it is also a broader category.

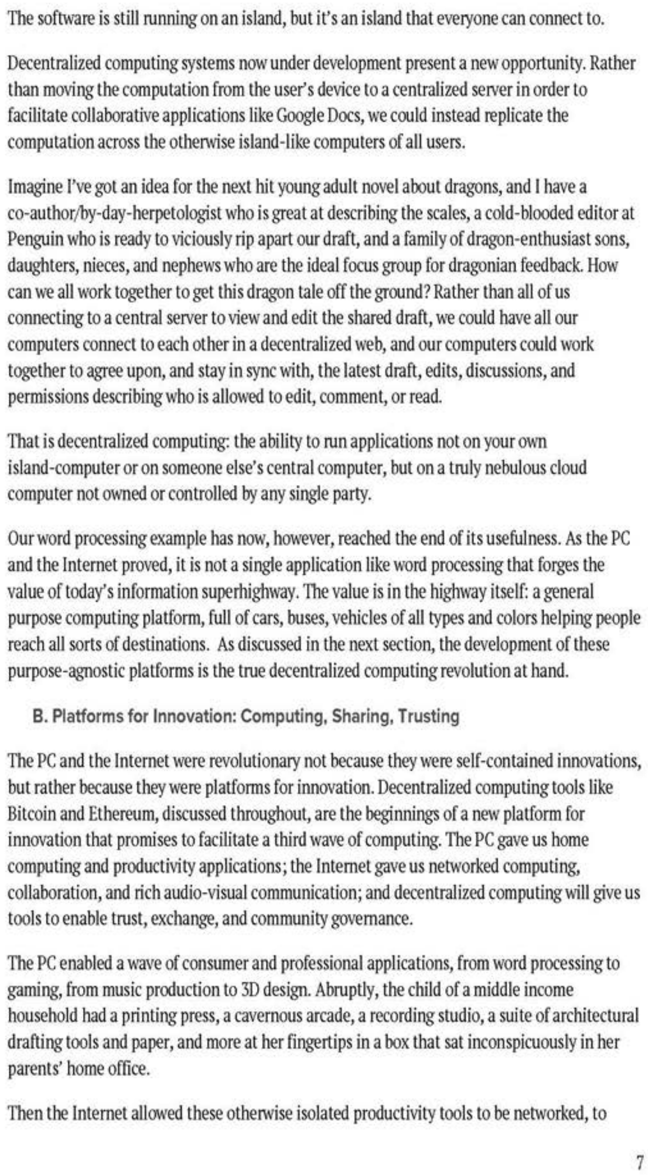
A. An Easy Introduction to Decentralized Computing

The easiest way to understand decentralized computing is to begin by thinking about a computer program you use and with which you are comfortable. It could be any computer program that you use for work or for fun. For this example, let's just pick a *word processor*. Sure it's not the most titillating software out there, but pretty much everyone who has ever used a computer has used a word processor at some point in their digital lives.

Let's think about the history of the word processor. In the *old* days—the 1990s no less—word processing, like dying, was something you always did alone. If you used Microsoft Word, Wordperfect, or MacWrite, you were running software that used *only* the processor, memory, disk space, monitor, and keyboard of *your personal computer*. The word processor was software trapped on an island. If you wanted to share your draft for the next great American novel, then you would either need to print it or save it as a file on a disk and hope your editor, reader, or critic had the same word processing software as you and could open the file on her own island-like computer. If she made edits she would need to send the file back and you would need to merge her changes with any changes you had made since she got a copy. Frustrating, but a real improvement over piles of redlined paper.

Fast forward to the 21st century and new word processing applications began to make collaboration easier, most notably Google Docs and Microsoft Word with OneDrive. These new services took advantage of what marketing executives persuasively and reassuringly dubbed "the cloud." Word processing via the cloud means it is much easier to work with others in creating a document; in the best implementations you can control who has read or write access, see your co-authors typing in real time, comment and discuss changes, and see a full history of everyone's edits.

From a computing standpoint this is not cloud magic. What is really happening is that the word processor software is no longer running on your island-like computer; it is running on a server that Google or Microsoft owns and maintains somewhere in a giant warehouse somewhere in the world. The interface that we see on our computers when we use these services is just that, an interface—a way to communicate with the computer that Google or some other cloud services provider owns and controls. Collaboration is a cinch with these systems because every editor can have an interface that talks to the same central computer.



The software is still running on an island, but it's an island that everyone can connect to.

Decentralized computing systems now under development present a new opportunity. Rather than moving the computation from the user's device to a centralized server in order to facilitate collaborative applications like Google Docs, we could instead replicate the computation across the otherwise island-like computers of all users.

Imagine I've got an idea for the next hit young adult novel about dragons, and I have a co-author/by-day-herpetologist who is great at describing the scales, a cold-blooded editor at Penguin who is ready to viciously rip apart our draft, and a family of dragon-enthusiast sons, daughters, nieces, and nephews who are the ideal focus group for dragonian feedback. How can we all work together to get this dragon tale off the ground? Rather than all of us connecting to a central server to view and edit the shared draft, we could have all our computers connect to each other in a decentralized web, and our computers could work together to agree upon, and stay in sync with, the latest draft, edits, discussions, and permissions describing who is allowed to edit, comment, or read.

That is decentralized computing: the ability to run applications not on your own island-computer or on someone else's central computer, but on a truly nebulous cloud computer not owned or controlled by any single party.

Our word processing example has now, however, reached the end of its usefulness. As the PC and the Internet proved, it is not a single application like word processing that forges the value of today's information superhighway. The value is in the highway itself: a general purpose computing platform, full of cars, buses, vehicles of all types and colors helping people reach all sorts of destinations. As discussed in the next section, the development of these purpose-agnostic platforms is the true decentralized computing revolution at hand.

B. Platforms for Innovation: Computing, Sharing, Trusting

The PC and the Internet were revolutionary not because they were self-contained innovations, but rather because they were platforms for innovation. Decentralized computing tools like Bitcoin and Ethereum, discussed throughout, are the beginnings of a new platform for innovation that promises to facilitate a third wave of computing. The PC gave us home computing and productivity applications; the Internet gave us networked computing, collaboration, and rich audio-visual communication; and decentralized computing will give us tools to enable trust, exchange, and community governance.

The PC enabled a wave of consumer and professional applications, from word processing to gaming, from music production to 3D design. Abruptly, the child of a middle income household had a printing press, a cavernous arcade, a recording studio, a suite of architectural drafting tools and paper, and more at her fingertips in a box that sat inconspicuously in her parents' home office.

Then the Internet allowed these otherwise isolated productivity tools to be networked, to speak to the world. The PC ran applications, and the Internet enabled those applications to communicate globally, to be multi-user, to share data. Now the home printing press was matched with a fleet of newspaper delivery trucks; the arcade, still cavernous, was open to players across the world who could compete with each other; the recording studio came with a record label, trucks to ship vinyl, and stores to sell hits; the architectural tools came with virtual warehouses of objects, furniture, homes, and vehicles waiting to be built or even printed in 3D.

The Internet created a uniform mechanism for computers to speak to each other, but it did not create a uniform mechanism for verifiable agreement (what we might call "trust") between two or more computers and their two or more users. As cryptographer Nick Szabo has written:

> When we currently use a smartphone or a laptop on a cell network or the Internet, the other end of these interactions typically run on other solo computers, such as web servers. Practically all of these machines have architectures that were designed to be controlled by a single person or a hierarchy of people who know and trust each other. From the point of view of a remote web or app user, these architectures are based on full trust in an unknown "root" administrator, who can control everything that happens on the server: they can read, alter, delete, or block any data on that computer at will.[2]

We have come to call shared computing tools "cloud computing," but, marketing aside, *there is no cloud, there's just other people's computers*. So when, today, we engage in any sort of shared computing—whether it be social networking, collaborative document editing, shopping, online banking, or posting a video of our pets—we are utilizing the computers of an intermediary—whether it be Facebook, Google, Amazon, Bank of America, or YouTube respectively. Those intermediaries have control over everything that happens on their servers. They can see a wealth of our personal data and users trust them to only use and manipulate that data according to user instructions and in the best interest of users. Any agreement or level of trust between two users of a given intermediary's service—as when I sell my car to another eBay user, or recognize the positive eBay feedback and reputation of the prospective buyer—is established and maintained by that intermediary.

This architecture has been essential to the rise of the Internet and collectively we have benefited tremendously from the creation of these shared computing systems. It does, however, introduce a great deal of trust into consumer-business relationships; trust that can be misplaced and abused if an intermediary maliciously misuses their customer's data, fails to

[2] Nick Szabo, "The dawn of trustworthy computing" *Unenumerated* (Dec. 2014) http://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html. *See also* IBM Institute for Business Value, *Device Democracy: Saving the future of the Internet of Things* https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF ("The Internet was originally built on trust. In the post-Snowden era, it is evident that trust in the Internet is over. The notion of IoT solutions built as centralized systems with trusted partners is now something of a fantasy. Most solutions today provide the ability for centralized authorities, whether governments, manufacturers or service providers to gain unauthorized access to and control devices by collecting and analyzing user data.").

secure it from hackers, or profits unfairly from a user who is locked into the service and finds it difficult to migrate their data to a competing service provider.

New and emerging computing architectures can help forge trustworthy relationships directly between users without intermediaries. The most visible of these new systems thus far is Bitcoin, a peer-to-peer network protocol that allows users to hold and send provably scarce tokens (bitcoins) that can function like cash for the Internet. Electronic cash, however, is just one potential computing service that can be designed to be intermediary-less, to run across the computers of a decentralized network of users rather than on the centralized servers of a particular service provider.

At root, any shared computing system can be thought of as a single shared computer, a computer made up of computers. Bitcoin is, following this logic, a computer made up of many computers whose several users have installed and are running Bitcoin-compatible software. Working together, all of these computers periodically come to an agreement over the ledger of all Bitcoin transactions—the Bitcoin blockchain. That ledger is, at any moment, the authoritative "state" of the decentralized Bitcoin computer. But computer "state" can be any data, not just a list of cash-like transactions. For example, when using Microsoft Word, a writer is perpetually updating the state of her computer, typing word after word into a document whose current changes—the current state—continually appear on the screen.

If a decentralized network of computers can continuously agree on the most recent and updated state of all interactions on that network—like keystrokes to a Word document—then it could be programmed to perform the computations necessary for any number of applications. Tracking the reputation of sellers and buyers, permissioning editing or access rights to a shared document, rewarding creative contributors for popular video content, any of the previously described "cloud" services provided by intermediaries could be programmed into a decentralized computing network. As Szabo has noted,

> Much as pocket calculators pioneered an early era of limited personal computing before the dawn of the general-purpose personal computer, Bitcoin has pioneered the field of trustworthy computing with a partial block chain computer. Bitcoin has implemented a currency in which someone in Zimbabwe can pay somebody in Albania without any dependence on local institutions, and can do a number of other interesting trust-minimized operations, including multiple signature authority. But the limits of Bitcoin's language and its tiny memory mean it can't be used for most other fiduciary applications[.][3]

Several efforts are underway to design systems that can enable a larger range of "fiduciary" applications, systems that will be effectively *general purpose decentralized computers*: platforms for trustworthy shared computing just as flexible and repurposable as the PC and the Internet have become. Some of these systems modify or build on top of Bitcoin (Rootstock[4] and

[3] *Id.*

[4] Sergio Demian Lerner, *RSK Rootstock Platform: Bitcoin Powered Smart Contracts* (Nov. 2015)

Blockstack[5] among others), others are new standalone network protocols (the largest by value is Ethereum[6]). Still others are building decentralized computing systems that are private or permissioned by default (most notably Corda by R3CEV[7]), in order to allow a pre-specified set of users to agree upon some limited-purpose computation—like validating contracts between banks.

The component parts of these new architectures are generally three-fold: peer-to-peer networking, blockchains, and consensus mechanisms. All three of these concepts are often lumped together under the general and impressive-sounding heading "blockchain technology," but for clarity this testimony will deal with each separately and will ultimately focus on the third lump—consensus mechanisms—because it is the architecture of this third component that has the most important implications for building useful and well-functioning decentralized applications.

You can think of these three technologies as follows: *peer-to-peer networking* is how connected machines communicate with each other, *blockchains* are the data structures the connected peers use to store important variables in the shared computation, and the *consensus mechanism* is the tool to generate the shared and agreed-upon computation itself.

As we will discuss, the architecture of the consensus mechanism is important to consider. Different choices may have different outcomes for users—more or less privacy, more or less choice, more or less costs to participation. Just as the fundamental technical architecture of the PC and the Internet had long-term ramifications for the relative fairness, distribution and availability of computing and communication tools, so may choices in the now-unfolding architecture of consensus.

As we will explain, *all* new approaches to decentralized computing—whether private or public—should be celebrated and allowed to develop relatively unfettered by regulatory or government policy choices much as the Clinton Administration took a light-touch approach to the development of the Internet in the 1990s.[8] In order to make those choices, however,

https://uploads.strikinglycdn.com/files/90847694-70f0-4668-ba7f-dd0c6b0b00a1/RootstockWhitePaperv9-Overview.pdf

[5] Muneeb Ali, Jude Nelson, Ryan Shea and Michael J. Freedman, *Blockstack: A Global Naming and Storage System Secured by Blockchains* (June 2016) https://blockstack.org/blockstack.pdf

[6] Vitalik Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform* (Jan. 2014) https://github.com/ethereum/wiki/wiki/White-Paper

[7] Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn, *Corda: An Introduction* (Aug. 2016) https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda2fdebbd1acc9c0309b2/1472045822585/corda-introductory-whitepaper-final.pdf

[8] President William J. Clinton, Vice President Albert Gore, Jr. *A Framework For Global Electronic Commerce* (July 1997) *available at* https://www.w3.org/TR/NOTE-framework-970706#Annotated Version ("Governments can have a profound effect on the growth of commerce on the Internet. By their actions, they can facilitate electronic trade or inhibit it. Knowing when to act and -- at least as important -- when not to act, will be crucial to the development of electronic commerce.5 This report articulates the Administration's vision for the emergence of the GII as a vibrant global marketplace by suggesting a set of principles, presenting a series of policies, and establishing a road map for international discussions and agreements to facilitate the growth of commerce on the Internet.")

policymakers need a basic understanding of how consensus works and what it might help us build.

C. Platforms for Innovation: Public or Private

A fundamental question in the design of any consensus mechanism is who can participate and how do they participate in order to reach consensus over some shared computation. For many years it was assumed that useful consensus mechanisms could only be developed if the participant computers were identified through channels outside of the decentralized computing system itself.[9] In other words, it had been assumed that useful consensus mechanisms could only be designed as private or permissioned systems: to participate in the decentralized computing system a user would need to either (a) gain physical access to a private underlying network architecture (*e.g.*, an "intranet" rather than the Internet) or (b) obtain an access credential via a cryptographic key exchange with other participants or by utilizing a public key infrastructure.[10] Several such private consensus mechanisms have been, and are continuing to be, developed.[11]

Private consensus mechanisms, however, may not be optimal for the development of robust

[9] *See* Jonathan Katz, Andrew Miller, and Elaine Shi, "Pseudonymous Broadcast and Secure Computation from Cryptographic Puzzles" (Oct 2014) *available at* http://eprint.iacr.org/2014/857.pdf ("Standard models of distributed computing assume authenticated point-to point channels between parties, where authentication may be provided via some physical property of the underlying network or using keys shared by the parties in advance. When security against a large fraction of corruptions is desired, even stronger pre-existing setup—*e.g.*, a broadcast channel or a public-key infrastructure (PKI) with which broadcast can be implemented—is often assumed. Such setup may not exist in many interesting scenarios, especially open, peer-to-peer networks in which parties do not necessarily have any prior relationships, and can come and go as they please. Nevertheless, such setup is often assumed due to the prevailing belief that nothing "interesting" can be achieved without them, and in fact there are known impossibility results to this effect."). *See also* Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, and Tal Rabin. "Secure computation without authentication." *Advances in Cryptology—CRYPTO 2005*, pp. 361–377 (2005).

[10] *Id.*

[11] *See, e.g.*, Paxos, a widely used protocol for generating consensus across a set of unreliable processors. Marshall Pease, Robert Shostak, and Leslie Lamport, "Reaching Agreement in the Presence of Faults," 27 *Journal of the Association for Computing Machinery* 228–234 (April 1980). We will not discuss Paxos or related consensus mechanisms within this paper. These systems are generally fault tolerant only under an assumption that none of the nodes are actively attempting to undermine the consensus by sending malicious and deceptive data to other nodes. The ability to deliver a useful distributed computing service despite the presence of malicious and deceptive participants is known in computer science as "byzantine fault tolerance" or BFT. *See* Kevin Driscoll, Brendan Hall, et a*l*, "Byzantine Fault Tolerance, from Theory to Reality" 2788 Lecture Notes in Computer Science 235 (2003). There are BFT variants of Paxos, however, they do not scale effectively to large, highly distributed computing networks. *See* Marko Vukolic, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication," *IBM Research* ("This is true even for their crash-tolerant counterparts, i.e., replication protocols such as Paxos, Zab and Raft, which are used in many large scale systems but practically never across more than a handful of replicas."). Accordingly, Paxos is a useful tool for generating an agreement amongst several computers all under one individual or institution's control. The technologies discussed in this paper are limited to newer mechanisms, inspired by Bitcoin, that seek explicitly to generate agreement amongst a large number of computers controlled by mutually distrustful strangers.

general purpose decentralized computing systems. Access to dedicated network infrastructure and/or public key infrastructure is costly, potentially limiting participation to larger players like businesses. In some cases, these prerequisites are irreconcilable with the desired decentralized computing use case, as when consensus is sought across a peer-to-peer network that allows peers free entry and exit.[12] If, as described in the previous section, we believe that some decentralized computing systems should be public platforms for democratic and diverse innovation (as were the PC and the Internet), then a permissioned system seems like a poor choice.

Private systems may be the smarter choice for limited rather than general purpose decentralized computing tasks, where consensus need not be open to all potential participants and participants can be centrally identified and trusted not to collude against the interests of the group (*e.g.*, when a consortium of banks wants to settle inter-bank loans according to a decentralized ledger).[13] Permissionless systems are arguably more difficult to scale,[14] to make private,[15] or to secure than private systems.[16] These, however, are technical challenges that may prove to be fully surmountable.

Much of the current skepticism exhibited by proponents of simpler, private systems could prove shortsighted. Similar issues of scale and usability clouded early predictions about computing generally. For example, in 1951 Cambridge mathematician Douglas Hartree suggested that "all the calculations that would ever be needed in [the UK] could be done on three digital computers—one in Cambridge, one in Teddington, and one in Manchester. No one else would ever need machines of their own, or would be able to afford to buy them."[17] Similar skepticism stalked the early Internet. For example, in 1998 economist Paul Krugman wrote,

> The growth of the Internet will slow drastically, as the flaw in "Metcalfe's law"–which states that the number of potential connections in a network is proportional to the square of the number of participants–becomes apparent: most people have nothing to

[12] Katz, *supra* note 9.

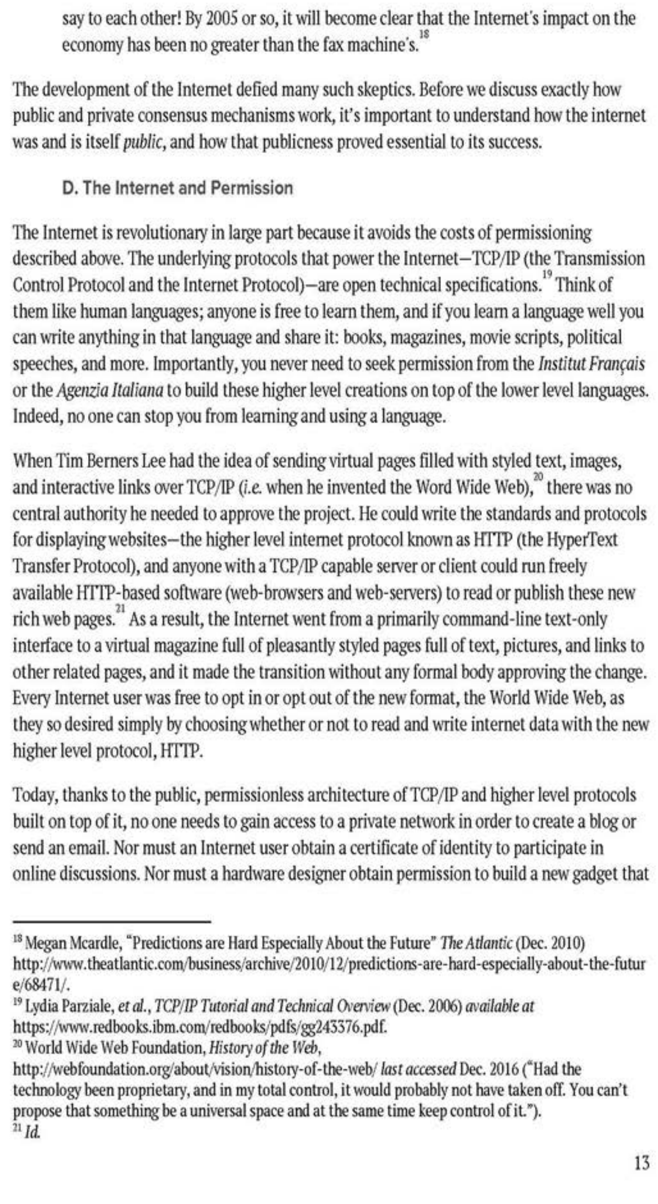
[13] *See, e.g.*, Gendal Brown, *supra* note 7.

[14] *See* Vukolic, *supra* note 11. *See also* Kyle Torpey, "Bitcoin Reaches a Crossroads With the Scaling Debate, Not a Crisis" *Bitcoin Magazine* (May 2016) https://bitcoinmagazine.com/articles/bitcoin-reaches-a-crossroads-with-the-scaling-debate-not-a-crisis-1462980183.

[15] *See infra* p. 35.

[16] *See* Robert Sams, "No, Bitcoin is not the future of securities settlement," (2015) http://www.clearmatics.com/2015/05/no-bitcoin-is-not-the-future-of-securities-settlement ("If you are prepared to use trusted third parties for authentication of the counterparts to a transaction, I can see no compelling reason for not also requiring identity authentication of the transaction validators as well. By doing that, you can ditch the gross inefficiencies of proof-of-work and use a consensus algorithm of the one-node-one-vote variety instead that is ... thousands of times more efficient.").

[17] Lord Bowden, 58 *American Scientist* 43 (1970). This accurate quotation is generally considered to be the basis for a notorious misquote of IBM President Thomas J Watson, "I think there is a world market for maybe five computers." Brader, Mark (July 10, 1985). "Only 3 computers will be needed..." (Forum post). https://groups.google.com/forum/#!msg/net.misc/390t08t_SZY/d2uJwCwcyQAJ.



> 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 machine's.[18]

The development of the Internet defied many such skeptics. Before we discuss exactly how public and private consensus mechanisms work, it's important to understand how the internet was and is itself *public*, and how that publicness proved essential to its success.

D. The Internet and Permission

The Internet is revolutionary in large part because it avoids the costs of permissioning described above. The underlying protocols that power the Internet—TCP/IP (the Transmission Control Protocol and the Internet Protocol)—are open technical specifications.[19] Think of them like human languages; anyone is free to learn them, and if you learn a language well you can write anything in that language and share it: books, magazines, movie scripts, political speeches, and more. Importantly, you never need to seek permission from the *Institut Français* or the *Agenzia Italiana* to build these higher level creations on top of the lower level languages. Indeed, no one can stop you from learning and using a language.

When Tim Berners Lee had the idea of sending virtual pages filled with styled text, images, and interactive links over TCP/IP (*i.e.* when he invented the Word Wide Web),[20] there was no central authority he needed to approve the project. He could write the standards and protocols for displaying websites—the higher level internet protocol known as HTTP (the HyperText Transfer Protocol), and anyone with a TCP/IP capable server or client could run freely available HTTP-based software (web-browsers and web-servers) to read or publish these new rich web pages.[21] As a result, the Internet went from a primarily command-line text-only interface to a virtual magazine full of pleasantly styled pages full of text, pictures, and links to other related pages, and it made the transition without any formal body approving the change. Every Internet user was free to opt in or opt out of the new format, the World Wide Web, as they so desired simply by choosing whether or not to read and write internet data with the new higher level protocol, HTTP.

Today, thanks to the public, permissionless architecture of TCP/IP and higher level protocols built on top of it, no one needs to gain access to a private network in order to create a blog or send an email. Nor must an Internet user obtain a certificate of identity to participate in online discussions. Nor must a hardware designer obtain permission to build a new gadget that

[18] Megan Mcardle, "Predictions are Hard Especially About the Future" *The Atlantic* (Dec. 2010) http://www.theatlantic.com/business/archive/2010/12/predictions-are-hard-especially-about-the-future/68471/.

[19] Lydia Parziale, *et al.*, *TCP/IP Tutorial and Technical Overview* (Dec. 2006) *available at* https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf.

[20] World Wide Web Foundation, *History of the Web*, http://webfoundation.org/about/vision/history-of-the-web/ *last accessed* Dec. 2016 ("Had the technology been proprietary, and in my total control, it would probably not have taken off. You can't propose that something be a universal space and at the same time keep control of it.").

[21] *Id.*

can send and receive data from the Internet.[22] This publicness has been a major factor in democratizing communications, and spurring vibrant competition and innovation. Anyone can design, build, and utilize hardware or software that will automatically connect to the Internet without seeking permission from a network gatekeeper, a national government, or a competitor.

It is true that businesses often utilize public key infrastructure online, and that this does add a layer of permissioning to the web. When you visit an online bank, for example, your web browser will look for a signed certificate issued by a *certificate authority* that has vouched for the bank's online identity.[23] This begins a process between your browser and the bank that will ultimately encrypt all of your communications while you are navigating the website. This process is known as TLS/SSL (Transport Layer Security and its predecessor, Secure Sockets Layer), and it is the system behind the little green lock consumers are told to watch out for when visiting sensitive websites like banks.[24]

TLS/SSL, however, is another application-layer Internet protocol—like HTTP—that runs *on top* of the public TCP/IP network. Again, the underlying protocols are the reason for the Internet's publicness. When a consumer device is connected to the Internet these protocols do not ask for identification, certificates, or authentication; they simply assign the new device a seemingly random but unique pseudonym (called an IP Address) in order to have a consistent address for routing data.[25] The identified and permissioned layer, TLS/SSL, is running on top of the public and pseudonymous layer.

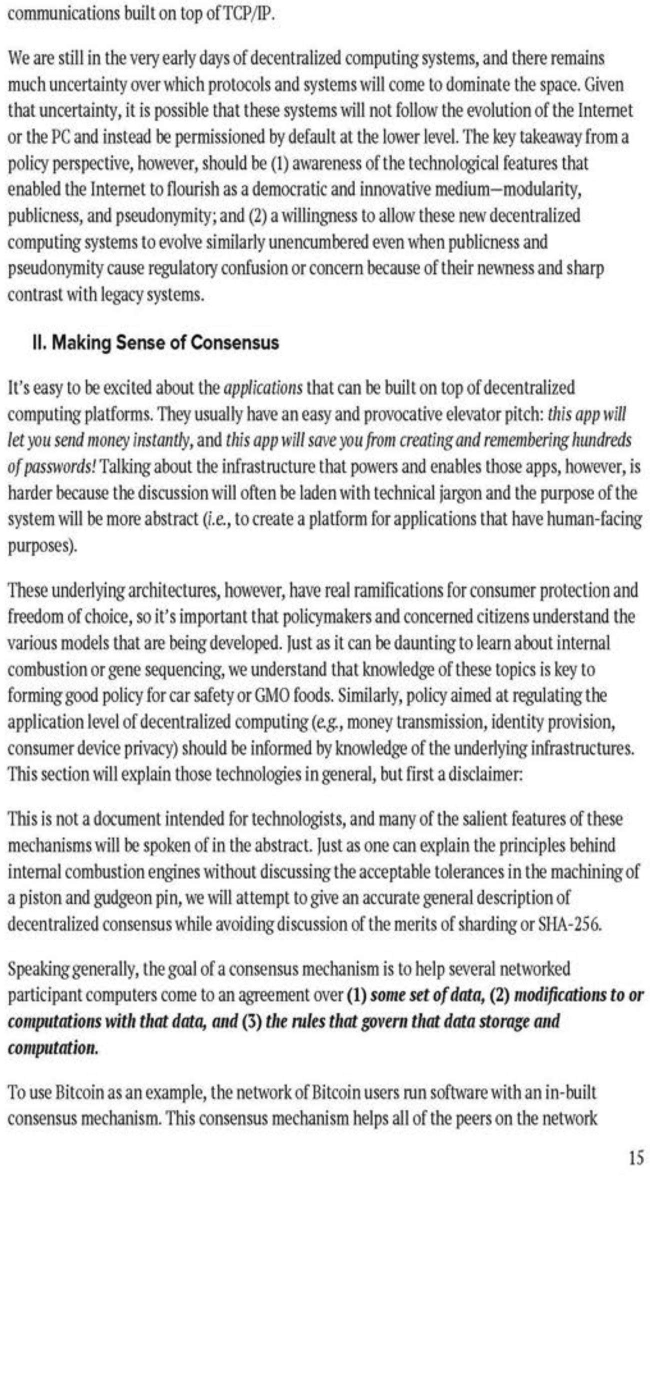
The layered design of the Internet is not accidental. It is modular, with a public lower layer, in order to enable flexibility. One can always build identified and permissioned layers on top of a permissionless system—as TLS/SSL (a private, identified layer) is built on top of TCP/IP (a public, pseudonymous layer). The reverse is not possible, however. Had the Internet originally been architected to be permissioned and identified, it would have imposed costs and limitations on public participation, and it would have ossified the possible range and diversity of future higher level protocols for identity and permission. When lower layers are permissionless and pseudonymous, on the other hand, the costs of participating are low (merely the cost of hardware and free Internet-protocol-ready software), and such a open platform enables a variety of private or identified higher level layers to emerge and compete for particular use cases where identity and permissioning are essential. For example, PGP and the Web of Trust compete with TLS/SSL as methods for enabling secure and identified

[22] *Id. See also* W3C, *Web of Devices* https://www.w3.org/standards/webofdevices/ *last accessed* Dec. 2016. ("W3C is focusing on technologies to enable Web access anywhere, anytime, using any device. This includes Web access from mobile phones and other mobile devices as well as use of Web technology in consumer electronics, printers, interactive television, and even automobiles.").

[23] Microsoft, *What is TLS/SSL?* (Mar. 2003) https://technet.microsoft.com/en-us/library/cc784450(v=ws.10).aspx.

[24] Google, *Check Chrome's connection to a site* https://support.google.com/chrome/answer/95617?hl=en *last accessed* Dec. 2016.

[25] *See* Stephanie Crawford, "What is an IP address?" *How Stuff Works* http://computer.howstuffworks.com/internet/basics/question549.htm *last accessed* Dec. 2016.



communications built on top of TCP/IP.

We are still in the very early days of decentralized computing systems, and there remains much uncertainty over which protocols and systems will come to dominate the space. Given that uncertainty, it is possible that these systems will not follow the evolution of the Internet or the PC and instead be permissioned by default at the lower level. The key takeaway from a policy perspective, however, should be (1) awareness of the technological features that enabled the Internet to flourish as a democratic and innovative medium—modularity, publicness, and pseudonymity; and (2) a willingness to allow these new decentralized computing systems to evolve similarly unencumbered even when publicness and pseudonymity cause regulatory confusion or concern because of their newness and sharp contrast with legacy systems.

II. Making Sense of Consensus

It's easy to be excited about the *applications* that can be built on top of decentralized computing platforms. They usually have an easy and provocative elevator pitch: *this app will let you send money instantly*, and *this app will save you from creating and remembering hundreds of passwords!* Talking about the infrastructure that powers and enables those apps, however, is harder because the discussion will often be laden with technical jargon and the purpose of the system will be more abstract (*i.e.*, to create a platform for applications that have human-facing purposes).

These underlying architectures, however, have real ramifications for consumer protection and freedom of choice, so it's important that policymakers and concerned citizens understand the various models that are being developed. Just as it can be daunting to learn about internal combustion or gene sequencing, we understand that knowledge of these topics is key to forming good policy for car safety or GMO foods. Similarly, policy aimed at regulating the application level of decentralized computing (*e.g.*, money transmission, identity provision, consumer device privacy) should be informed by knowledge of the underlying infrastructures. This section will explain those technologies in general, but first a disclaimer:

This is not a document intended for technologists, and many of the salient features of these mechanisms will be spoken of in the abstract. Just as one can explain the principles behind internal combustion engines without discussing the acceptable tolerances in the machining of a piston and gudgeon pin, we will attempt to give an accurate general description of decentralized consensus while avoiding discussion of the merits of sharding or SHA-256.

Speaking generally, the goal of a consensus mechanism is to help several networked participant computers come to an agreement over **(1) *some set of data,* (2) *modifications to or computations with that data, and* (3) *the rules that govern that data storage and computation.***

To use Bitcoin as an example, the network of Bitcoin users run software with an in-built consensus mechanism. This consensus mechanism helps all of the peers on the network

(Bitcoin users):

1. ***Store agreed-upon data:*** every peer gets a copy of the full ledger of all bitcoin transactions in the history of the network.
2. ***Compute and transform that data:*** recipients of bitcoin transactions can write new transactions thus adding to the ledger all transactions.
3. ***Agree on rules for how storage and computation of that data can take place:*** the ledger is continually updated because all peers listen for and relay new transactions if they are valid, and a lottery is used to periodically pick a random peer to state the authoritative order of valid transactions for chunks of time that are about 10 minutes long. (There are other rules but these are probably the most general and fundamental Bitcoin consensus rules).

If this example is not entirely clear, that's OK. We will expand upon it later in this testimony. The key thing to remember is that *consensus* means that a network of peers can agree upon three things: **(1)** ***data,*** **(2)** ***computation (transformation of the data), and*** **(3)** ***the rules for how computation can take place***.

Any particular *consensus* mechanism can be designed to leverage two techniques in order to ensure agreement over a computation and the associated data.

First, there are what we can call ***automatic rules***. To use an automatic rule, all parties to the consensus can run software on their computers that automatically rejects certain "invalid" computational operations or outcomes on sight. To make a legal analogy, we can think of this as *res ipsa loquitur* (the principle that the mere occurrence of an accident implies negligence), or a rule of strict liability.

For example, Bitcoin's core software defines certain outcomes as always impermissible on sight. Most notably, transactions from one user to another cannot send any bitcoins that have not previously been sent to the sender.[26] More simply: I can't hand you cash that hasn't previously been given to me. To be compatible with the larger Bitcoin network, the software you run on your computer *must follow this rule*. If it does not, other nodes on the network will ignore any invalid messages you send using it. You can try to send the network messages that attempt such counterfeiting, but your messages will always fall on deaf ears and the effort will be futile. These are automatic rules that help the network ignore data that is irrelevant or malevolent to the agreement the participants are seeking.

Second, there are what we can call ***decision rules***. In situations where there are two differing outcomes from the computation, but where both would be valid based on the automatic rules, a rule of decision between each possible valid state is needed in order to keep the network in agreement. All parties to the consensus can agree in advance (by choosing which software to run) to always honor one possible valid outcome over another possible valid outcome based on a decision rule. From a legal perspective this is more like a judgement of fact from a jury at

[26] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nov. 2008) p. 2 https://bitcoin.org/bitcoin.pdf.

trial.

For example, Bitcoin's core software does not tell you when any particular valid transaction comes before another valid transaction in the order-keeping ledger of all historical transactions. This order is, nonetheless, critical to determine who paid whom first. Instead of using an automatic rule to settle uncertainties regarding transaction order, Bitcoin's software specifies a decision rule to resolve debates over which valid transaction came first.[27] Specifically, the Bitcoin software calls for a *repeated leader election by proof-of-work*, which we will discuss in a moment while outlining proof-of-work consensus. For now, it's important to simply understand that there are various ways of establishing a decision rule in order to reach consensus over the authoritative state of a decentralized computing system when multiple valid states are possible. All currently employed methods fall into four broad categories: (A) proof-of-work, (B) proof-of-stake, (C) consortium consensus, and (D) social consensus.

A. Proof-of-Work

As just mentioned, Bitcoin employs a *proof-of-work leader election* as the decision rule for determining the order of valid transactions in the blockchain. Such a consensus method might be useful for various decentralized computing systems, but Bitcoin allows us to describe a working example. *Leader election* means that one participant's record of which transactions came first, second, third, *etc.,* will be selected by all other network participants as the authoritative order of transactions for some designated period of time (beginning with that participant's successful election as leader and ending with the next leader election). We can see how this is a rule of decision, it says essentially: *whenever there is disagreement over two alternative but valid outcomes, defer to the chosen leader's choice for the given period.*

Proof-of-work is the specific method found in the Bitcoin protocol that describes how a leader is periodically chosen.[28] The proof-of-work system is essential to keeping the consensus mechanism *public.* This "election" is, therefore, not anything like the democratic political process to which we are accustomed. After all, if users come and go, freely connecting to the public network without identifying themselves, how would we ever keep track of who is who, or who is trustworthy and deserves our vote? So instead of having a vote, the network holds a lottery where there will be a random drawing and a winner every so often (roughly every 10 minutes for Bitcoin and every 12 seconds for Ethereum).[29]

The term *leader election* is the correct computer science term for this architecture,[30] but for the

[27] *Id.* at 2-3.

[28] *See* Nakamoto *supra* note 26 at 3 ("The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs").

[29] *See* Vitalik Buterin, "Toward a 12-second Block Time" *Ethereum Blog* (July 2014) https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/.

[30] *See* Indranil Gupta, Robbert van Renesse, and Kenneth P. Birman, "A Probabilistically Correct Leader Election Protocol for Large Groups," *Technical Report, Cornell University* (April 2000) ("The classical specification of the leader election problem for a process group states that at the termination of the

rest of us that sounds like something that involves voting and majorities rather than probabilities and lotteries. For clarity we will use the term *leader lottery* from here onwards.

Selecting a periodic leader via lottery in the real world would be easier than finding one on a peer-to-peer network. We could all meet in a room, introduce ourselves, and make it real simple by having everyone put their names in a hat and have one blindfolded person pull out a winner.

That simplicity doesn't work online. If all our peers on the network are putting names in a digital hat, we have no idea if each digital name matches one-to-one with a real person.[31] We could reasonably expect some less-than-scrupulous individuals to make up a bunch of random fake names and stick them in the hat. In the digital world we'd have no way of knowing whether Alice, Beth, Chuck, Dana, and Eve are each real individuals or merely pseudonyms (*i.e.*, "sock puppets") made up by Alice in order have a better chance at winning the lottery. We could try to employ some digital identity system to stop that fraud, but then we would be relying on an external identifier to guarantee the fairness of the system, and that defeats the point of having a public, ungated system to begin with. It would make it costly to participate because you would need to get identified in the real world to do your computing on the decentralized network, and it would force everyone to place trust in the identifier.

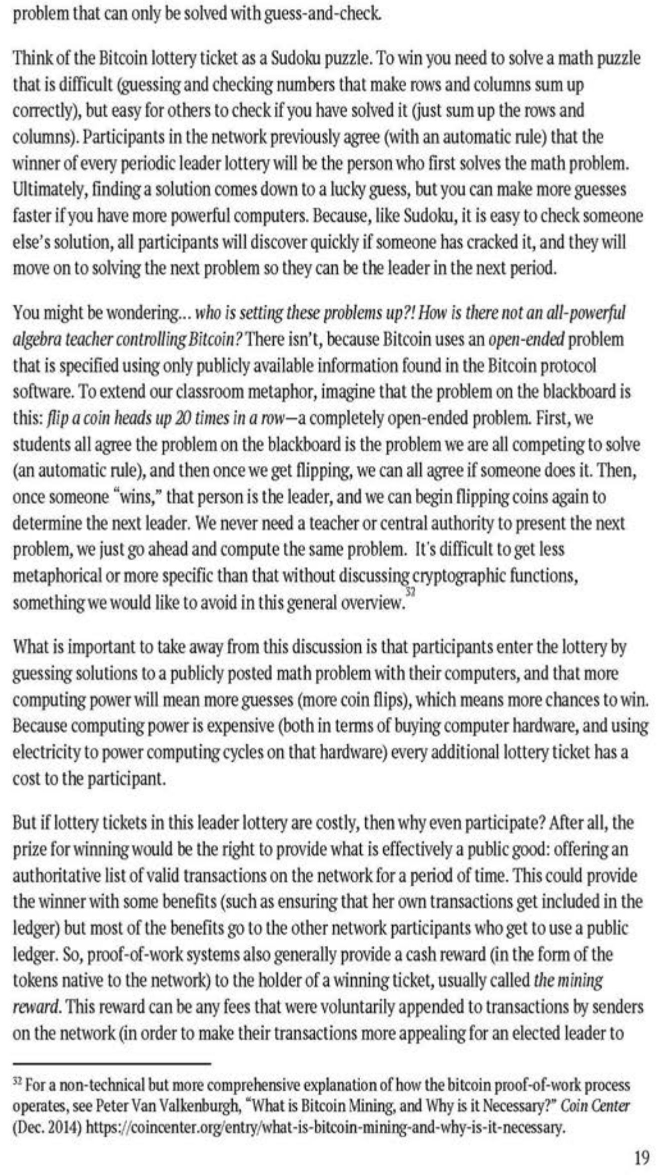
Rather than identify all lottery participants and pick names from a hat, we could have a ticket-based lottery, like Powerball. These lotteries only work if the lottery tickets have a cost (if they were free how many tickets to the Powerball would you claim for yourself?). A proof-of-work consensus system merely seeks to make it costly to enter yourself in the lottery. So Alice could still have more than one chance to win, but she incurs real costs every time she buys a new chance.

This has two desirable consequences that help make the lottery a good tool for selecting periodic leaders in a consensus mechanism. (1) *Decentralization:* It would be prohibitively costly to amass enough tickets to ensure that you would be the periodic leader for many repeated periods. (2) *Skin-in-the-game:* Leaders tend to be participants who have made sizable investments in the system by buying costly tickets. Generally speaking, the first reduces the capacity for self-dealing (always putting your transactions first), and the second ensures that the costs of malfeasance are internalized by the participants (who have invested real capital in the long-term success of the platform).

But how do we make those tickets costly when there is no central authority to verify payment? A proof-of-work consensus mechanism imposes costs on participants by making every ticket costly as measured in computing power that provably performs some "work," hence the name proof-of-work. Effectively, every lottery ticket costs one attempt at solving a difficult math

protocol, exactly one non-faulty group member is elected as the leader, and every other non-faulty member in the group knows about this choice.").

[31] *See* Nakamoto *supra* note 26 at 3 ("If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs").



problem that can only be solved with guess-and-check.

Think of the Bitcoin lottery ticket as a Sudoku puzzle. To win you need to solve a math puzzle that is difficult (guessing and checking numbers that make rows and columns sum up correctly), but easy for others to check if you have solved it (just sum up the rows and columns). Participants in the network previously agree (with an automatic rule) that the winner of every periodic leader lottery will be the person who first solves the math problem. Ultimately, finding a solution comes down to a lucky guess, but you can make more guesses faster if you have more powerful computers. Because, like Sudoku, it is easy to check someone else's solution, all participants will discover quickly if someone has cracked it, and they will move on to solving the next problem so they can be the leader in the next period.

You might be wondering... *who is setting these problems up?! How is there not an all-powerful algebra teacher controlling Bitcoin?* There isn't, because Bitcoin uses an *open-ended* problem that is specified using only publicly available information found in the Bitcoin protocol software. To extend our classroom metaphor, imagine that the problem on the blackboard is this: *flip a coin heads up 20 times in a row*—a completely open-ended problem. First, we students all agree the problem on the blackboard is the problem we are all competing to solve (an automatic rule), and then once we get flipping, we can all agree if someone does it. Then, once someone "wins," that person is the leader, and we can begin flipping coins again to determine the next leader. We never need a teacher or central authority to present the next problem, we just go ahead and compute the same problem. It's difficult to get less metaphorical or more specific than that without discussing cryptographic functions, something we would like to avoid in this general overview.[32]

What is important to take away from this discussion is that participants enter the lottery by guessing solutions to a publicly posted math problem with their computers, and that more computing power will mean more guesses (more coin flips), which means more chances to win. Because computing power is expensive (both in terms of buying computer hardware, and using electricity to power computing cycles on that hardware) every additional lottery ticket has a cost to the participant.

But if lottery tickets in this leader lottery are costly, then why even participate? After all, the prize for winning would be the right to provide what is effectively a public good: offering an authoritative list of valid transactions on the network for a period of time. This could provide the winner with some benefits (such as ensuring that her own transactions get included in the ledger) but most of the benefits go to the other network participants who get to use a public ledger. So, proof-of-work systems also generally provide a cash reward (in the form of the tokens native to the network) to the holder of a winning ticket, usually called *the mining reward*. This reward can be any fees that were voluntarily appended to transactions by senders on the network (in order to make their transactions more appealing for an elected leader to

[32] For a non-technical but more comprehensive explanation of how the bitcoin proof-of-work process operates, see Peter Van Valkenburgh, "What is Bitcoin Mining, and Why is it Necessary?" *Coin Center* (Dec. 2014) https://coincenter.org/entry/what-is-bitcoin-mining-and-why-is-it-necessary.

include in the section of the ledger she is writing), as well as permission within the software's automatic rules to create new money by sending herself a transaction with no source of funds (socializing the cost of a reward through inflation).[33]

Bitcoin users who decide to participate in this leader lottery have come to be called Miners because they perform "work" in return for newly created value. The label, however, belies the larger role these participants play in generating and maintaining consensus across the decentralized computing system. Both the work and the reward are secondary technical features necessary to the creation of a decentralized mechanism for picking periodic leaders who can ensure that data discrepancies between participants are quickly and fairly resolved.

Without a reward baked into the conesus mechanism, it is hard to understand why users would be incentivized to participate honestly in maintaining the network. Much fuss has been made over developing a "blockchain without the bitcoin," as if the currency aspect of the network pollutes what would otherwise be a useful network technology with an ideology or political agenda (or, at the very, least creates too many regulatory complications to be worth the trouble). But, as we can see, the only way to maintain a public network where leaders need to be periodically selected and rewarded for their participation is to award them with tokens that are native to the network itself (*i.e.*, the transaction history and scarcity of the token are a part of the data over which the consensus network is continually coming to an agreement). If participants are rewarded with assets that exist only according to data structures outside the network (*e.g.*, dollars or yen, the balances and scarcity of which are described in the balance sheets of banks) then we've reintroduced the need for identified parties who must be trusted to perform the rewarding function honestly and without bias.

Public blockchain networks need scarce tokens for technical reasons, not (merely) because their proponents may have political or ideological motivations for supporting alternative currencies. Ethereum, for example, is a public consensus-driven decentralized computing network that aspires to provide several user applications aside from electronic cash (*e.g.*, identity management,[34] reputation accounting,[35] community governance,[36] etc.), but it still has

[33] Recall that this is a violation of the automatic rule we discussed earlier in Bitcoin—this is the one exception to that automatic rule, you can send funds without referencing a funding source if and only if you won the leader lottery for the period when you send the transaction; this special transaction is called a coinbase transaction and the amount you are allowed to send is capped according to the monetary policy of the cryptocurrency—yet another automatic rule in the software.

[34] *See, e.g.*, Thomson Reuters, *BlockOneID for Ethereum: An identity mapping service for Ethereum blockchains*, https://blockone.thomsonreuters.com/ *last accessed* Dec. 2016.

[35] *See, e.g.*, Jack Peterson and Josephf Krug, *Augur: a Decentralized, Open-Source Platform for Prediction Markets*, http://bravenewcoin.com/assets/Whitepapers/Augur-A-Decentralized-Open-Source-Platform-for-Prediction-Markets.pdf.

[36] *See* Vitalik Buterin, "An Introduction to Futarchy" *Ethereum Blog* (Aug. 2014) https://blog.ethereum.org/2014/08/21/introduction-futarchy/ ("Although our modern communications technology is drastically augmenting individuals' naturally limited ability to both interact and gather and process information, the governance processes we have today are still dependent on what may now be seen as centralized crutches and arbitrary distinctions such as 'member', 'employee', 'customer' and

a scarce token that rewards winning participants in the leader lottery: ether. A blockchain without bitcoin or similarly scarce token is a private network, essentially a shared database with pre-identified and authenticated users.

To recap, a public consensus method should allow anyone to participate without obtaining some sort of credential from an external identifier. Without identification, however, a user could pretend to be several users and gain an unfair advantage in the leader lottery used to reach agreement when there are disputes over two or more valid outcomes (like alternative orders of transactions in a ledger). To deal with this problem, participation in the leader lottery is made costly by demanding that participants solve difficult math equations that will require costly hardware and electricity—proof-of-work. As a result, it (A) becomes too expensive to dominate the lottery by obtaining a substantial number of tickets, and (B) ensures that lottery winners are invested in the long-term success of the decentralized computing system. Winning participants are, in turn, rewarded with a scarce token native to the network.

B. Proof-of-Stake

Now that we have an intuitive understanding of proof-of-work consensus, it is fairly simple to explain the general mechanism behind proof-of-stake consensus. Recall that the goal behind proof-of-work is to make participation in the consensus costly. If the consensus mechanism involves a leader lottery, then we employ proof-of-work to make buying up all the lottery tickets prohibitively expensive.

Proof-of-stake systems are also designed to make participation come at the cost of some provable sacrifice. Instead of requiring calculation in exchange for a lottery ticket, a proof-of-stake mechanism requires that participants prove that they hold and/or can temporarily forgo access to a valuable token that travels on the network.[37] So if Bitcoin was a proof-of-stake-based cryptocurrency, then participation in the lottery could require users to stake some of the bitcoins they control—to prove that they control or to sacrifice their control over those valuable funds. The mechanism could demand that participation requires merely a mathematical proof that the user has possession of these tokens on the blockchain, or it could

'investor' – features that were arguably originally necessary because of the inherent difficulties of managing large numbers of people up to this point, but perhaps no longer. Now, it may be possible to create systems that are more fluid and generalized that take advantage of the full power law curve of people's ability and desire to contribute. There are a number of new governance models that try to take advantage of our new tools to improve transparency and efficiency, including liquid democracy and holacracy; the one that I will discuss and dissect today is futarchy.").

[37] *See* Vitalik Buterin, "What proof of stake is and why it matters" *Bitcoin Magazine* (Aug 2013) https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463 ("Rather than requiring the prover to perform a certain amount of computational work, a proof of stake system requires the prover to show ownership of a certain amount of money. The reason why Satoshi could not have done this himself is simple: before 2009, there was no kind of digital property which could securely interact with cryptographic protocols. Paypal and online credit card payments have been around for over ten years, but those systems are centralized, so creating a proof of stake system around them would allow Paypal and credit card providers themselves to cheat it by generating fake transactions.").

demand the permanent relinquishment or even destruction of these token (something often referred to as "proof-of-burn"[38]), or it could be a temporary stake, effectively a bond (*e.g.*, I stake 50 bitcoins—and thereby relinquish my ability to spend them—for the next 150 cycles of the leader lottery at which point I will regain control over the coins and can decide whether to stake again in the future). Regardless of how exactly it is specified, the goal is to use the value of the tokens (rather than the cost of computing) as the provable signal necessary for participation in the leader lottery.

If the tokens that travel on this decentralized network are available for sale on a variety of competitive exchanges (whether in exchange for dollars, euros, or other cryptocurrencies) or can be obtained by free transfer from existing users (whether as a gift or in payment for labor or some valuable good) then anyone with sufficient economic resources can, in theory, join the consensus, because they can obtain the tokens necessary to offer a proof-of-stake. In this sense, proof-of-stake consensus methods are, like proof-of-work methods, public.

C. Consortium Consensus

Consortium systems have a simpler solution to making lottery-style elections fair: only allow identified parties to participate. If we decide to trust an outside authority to identify all consortium members, provisioning members with cryptographic keys which they can use to sign their communications and prove authenticity, then we can run software that would only grant lottery tickets to participants who send validly signed messages.[39] We know Alice, Beth, Chuck, Dana, and Eve are each real individuals because we previously provisioned them each

[38] *See* Counterparty, "Why Proof-of-Burn" *Counterparty Blog* (Mar. 2014) http://counterparty.io/news/why-proof-of-burn/.

[39] When all parties are identified and can be trusted we may not even need a provably fair leader lottery; the leader could simply be the consortium participant with the best quality connection to the network, or it could rotate according to a pre-established order, or an upcoming schedule of leaders could be picked by an offline meeting of participants every year. Indeed, the identified parties could simply choose to use one of the many pre-blockchain fault-tolerant consensus protocols, *e.g.* Paxos, which have a long (around 25 years) and established track record (*see* Pease *supra* note 11), or perhaps simply a basic distributed database tool, *e.g.* an Oracle Database product. It is the longstanding availability of these tools and their persistent non-adoption by the financial industry that has spurred many to cynically characterize the present enthusiasm for permissioned blockchains as nothing more than a bitcoin-inspired and blockchain-branded pitch for selling marginally improved infrastructure to conservative institutions. *See, e.g.*, Wences Casares, (Panel Remarks) *Tech Crunch Disrupt: Is it time to stick a fork in Bitcoin?* (Sep. 2015) https://www.youtube.com/watch?v=ORcFGBhDDis ("That's called a private database, and it has existed for a long time. What's new about Bitcoin is that it's a decentralized, trustless ledger. The second you do it your own it's called a private database, and they have existed for a very long time. There's nothing revolutionary about that. ... If you're a Visa executive, Bank of America executive, or a Wells Fargo executive, it has become very fashionable to say, 'I really, really like the blockchain. I'm very interested in the blockchain, but I'm not interested in bitcoin,' which is the equivalent of saying, 'I really like the browser, but I don't like the Internet.' It's ridiculous. Those people don't want to be the ones who didn't see the Internet coming, and they want to say something nice about it without saying something nice about it. They don't realize that the blockchain does not work without bitcoin. The blockchain is the first decentralized, trustless database because the miners maintain it, and the miners do so because they get paid in bitcoin. Even though there are a lot of nice use cases on top of that, none of them work without the miners being paid with bitcoin.")

with secret keys and to obtain a lottery ticket each signs a message with his or her unique key.

This consortium method avoids the costs of solving math problems or staking valuable tokens that is inherent in proof-of-work and proof-of-stake systems.[40] The consortium method, however, also reintroduces permission and trust into the decentralized computing system. We need to be identified and granted access to the network in order to participate and we need to trust that the party tasked with making these identifications is acting fairly.

D. Social Consensus

Finally, we come to the last general category of consensus mechanisms, social consensus. You can think of the social consensus mechanism as somewhere in between the fully identified and permissioned consortium model, and the fully pseudonymous and public proof-of-work and proof-of-stake models.

Like the consortium model, you choose to trust some identified participants rather than relying on pseudonymous participants who offer a costly signal of credibility. Unlike the consortium model, however, each individual is her own identifying authority; she can choose which counterparties she trusts and build a social network of those with whom she feels comfortable entrusting the role of writing new data to the blockchain (or agreeing on some computation generally). We might then expect various users with differing social networks to disagree over the authoritative state of the consensus data, but the network can be designed to come to global agreement by looking for a subset of all transaction or computation data that some minimum number of trusted participants (perhaps a majority or a supermajority of trusted participants on the network) have agreed upon.[41]

As with proof-of-work and proof-of-stake consensus mechanisms, a social consensus mechanism will generally be public. Anyone can join but they must be selected as trustworthy by some minimum number of participants before they can participate in full.

III. Publicness, Trust, and Privacy Across Various Consensus Models

We've spent a good deal of time outlining these various consensus models because the specifics of their architecture will inevitably have meaningful consequences for the applications that are built on top of them, and, by extension, the people who will use those applications. One does not simply procure some "blockchain technology" to build better digital identity systems, property registries, voting infrastructure, or any of the other ambitious killer apps that have been proposed and widely touted for this technology. Building

[40] *See* Sams *supra* note 16.

[41] *See, e.g.*, the Ripple Protocol's consensus mechanism. David Schwartz, Noah Youngs, Arthur Britto, *The Ripple Protocol Consensus Algorithm* (2014) https://ripple.com/consensus-whitepaper/ ("Each server, maintains a unique node list (UNL), which is a set of other servers that s queries when determining consensus. Only the votes of the other members of the UNL of s are considered when determining consensus (as opposed to every node on the network). Thus the UNL represents a subset of the network which when taken collectively, is "trusted" by s to not collude in an attempt to defraud the network.").

any of those applications will require either (A) the modification and use of an existing consensus network (*e.g.*, build the application on top of Bitcoin or Ethereum) or (B) the creation of a new consensus network (both the development of consensus software and the bootstrapping of a network of peers who run the software that generates the consensus). The choice of whether to use one of the existing *public* (*i.e.*, proof-of-work, proof-of-stake, or social consensus) networks, to create a new *public* network, or to design and implement a private consensus network will be a choice that affects the relative publicness of the application, the degree of trust that users must place in other users or maintainers of the application or the underlying network, and the degree of privacy that the application is capable of offering its users. Each of these key consensus mechanism attributes, publicness, trust, and privacy will now be discussed in turn.

A. Publicness Across Consensus Mechanisms

Speaking generally, public consensus-driven decentralized computing systems are exciting and disruptive because their publicness resembles the early Internet. As we described previously, the Internet became the vibrant ecosystem we know today largely because it is so easy to build hardware or software that can seamlessly integrate with TCP/IP, the lower level networking protocol (language) that powers the network. That lower level is pseudonymous. Devices connect to the network and are automatically assigned a seemingly random number rather than a real-world identity.[42] The lower level is permissionless. Devices can send or receive data to and from any other pseudonym so long as the messages conform to the protocol specification.[43] The lower level is general purpose and extensible. TCP/IP only describes how packets of data should move through the network. It does not dictate what the contents of those packets can or should be.[44] Higher level protocols can be built on top of TCP/IP to interpret sent data as web pages, links, videos, emails, SWIFT bank messages,[45] anything that can be imagined, invented, and digitized.

The similarity of TCP/IP to Bitcoin, Ethereum, or any other public blockchain network should be apparent. These systems are also pseudonymous. Users are assigned random but unique cryptographic addresses.[46] These systems are also permissionless. Users can read or write data to the blockchain at will, sending or receiving transactions without seeking the permission of any centralized party. And these systems are also general purpose and extensible. Several parties are building new applications and application layers on top of the Bitcoin network,[47]

[42] Crawford *supra* note 25.
[43] W3C *supra* note 21.
[44] *Id.*
[45] Starting in the late 90s several standardized bank messaging services and cooperatives transitioned or adapted their systems to utilize TCP/IP as an underlying networking protocol. SWIFT messages travel over SWIFTNet a higher level Internet protocol that runs on top of TCP/IP. Additionally, the network that supports Fedwire messages, FEDNET, and CHIPS (the international Clearing House Interbank Payment System) network are both built to run on top of TCP/IP. *See* Roy S. Freedman, ***Introduction to*** *Financial Technology* (Apr. 2006) pp. 241-246.
[46] Here is an example of a bitcoin address: 1CPwNACt62wts2yGbz1vUuqeGD58SzzeAL.
[47] *See, e.g.*, Lerner *supra* note 4, and Ali *supra* note 5.

and Ethereum is explicitly designed to be a flexible foundation for building any trust-minimized application.[48]

In the previous section we classified four types of consensus mechanism into two groups:

- **Public:** Proof-of-work, Proof-of-stake, Social Consensus
- **Private:** Consortium Consensus

Decentralized computing systems built using public consensus mechanisms will, in general, be available to any participants who have an internet-connected device and free software that is compatible with the network. Systems built using a private consensus mechanism will, in general, only be available to participants who have previously identified themselves offline and been granted some form of credential by the identifying authority, which they can use to authenticate their identity whenever they connect to the network.

This characterization of publicness lacks, however, an important nuance. There are basically only two things that any user or potential user might want to do with a decentralized computing network: (1) write data to the network and have it included in the consensus-derived data structure or blockchain, or (2) read data from that network's consensus-derived data structure. Accordingly, a Bitcoin user making a transaction is *writing* new data to the Bitcoin blockchain while a user who queries their balance to confirm payment receipt is *reading* data from the blockchain.

Some have characterized networks where users can freely write consensus data as "permissionless." That is in contrast to "permissioned" networks where users need off-network identification and authentication in order to write. Read access is then characterized as public (anyone can read consensus data) vs. private (only identified and authenticated participants can read consensus data). These terms, however, can be confusing (is a network that has public read-access but private write-access truly public?) so we will continue to use public only in cases where both reading and writing are open to general participation and private in all other cases. For clarity we can summarize this more nuanced characterization with a four-by-four matrix:

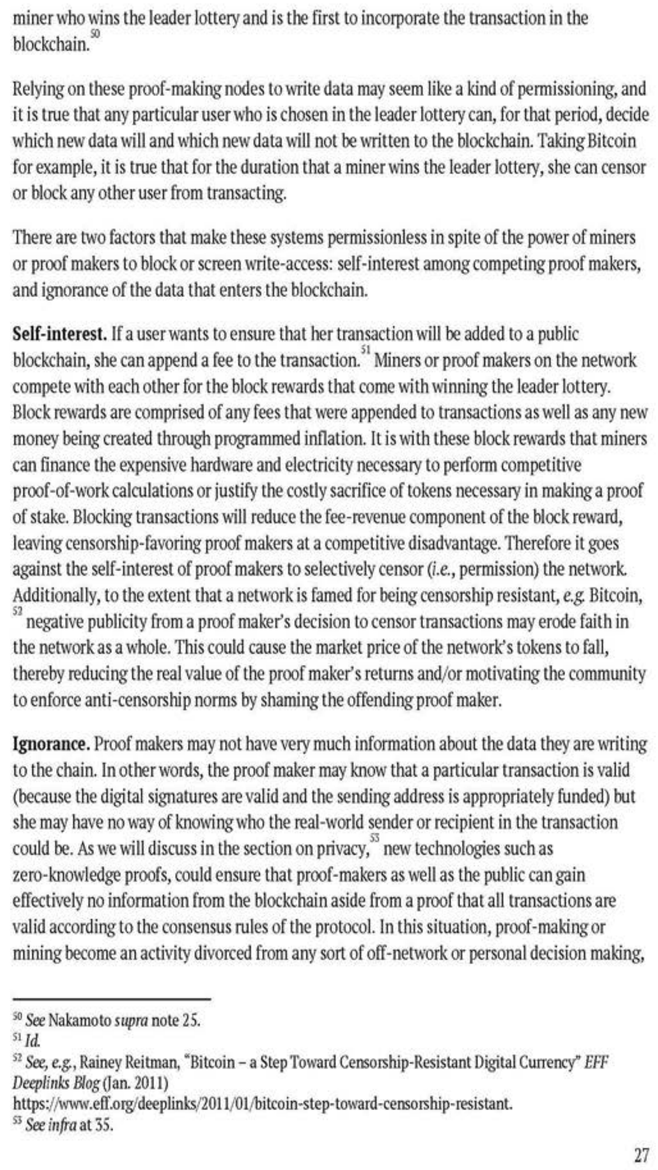
[48] *See* Buterin *supra* note 6.

		Writing Data Requires:	
		Internet-connected device, free software, and proof-of-work or proof-of-stake.	Off-network Identification, Authentication, and Permission.
Reading Data Requires:	Internet-connected device and free software.	Public (Permissionless, Public Blockchain)	Public for Reading, Private for Writing (Permissioned, Public Blockchain)
	Off-network Identification, Authentication, and Permission.	Public for Writing, Private for Reading (Permissionless, Private Blockchain)	Private (Permissioned, Private Blockchain)

Note an important subtlety in this chart. Public for reading is characterized as requiring only that the reader have an Internet-connected device and free software, while public for writing requires those things but also a proof, either of work or of stake. Bitcoin and Ethereum both exhibit this form of read/write publicness. Anyone with an Internet-connected device and free software can connect to these networks and download the full set of consensus data, *e.g.* the blockchain or list of all valid transactions made on the network from its start. Writing new data to these networks is not quite as easy. If one wants to truly be the node on the network that adds new data to the blockchain, one will have to be selected in the leader elections described in the previous section.[49] So, to truly write new data on these networks one must provide a proof (of computer work or of stake in the network's native token) and then be selected in the network's leader lottery. Even then, however, the user will only truly *write* data to the blockchain for those periods in which she has been chosen as leader.

This, however, is an overly pedantic description of who may write data on these networks. Thousands of people *do* write data to these public blockchain networks without ever running a node that makes a proof, *i.e.* mining. This is because anyone can send a new transaction message to various peers on the network and reasonably expect that the transaction will be picked up by a proof-making node, *i.e.* a miner, who will then incorporate it into a block of transactions which will then be added to the blockchain when that miner wins the leader lottery for a given period. Non-mining peers who want to ensure that their transaction will be written to the blockchain quickly can attach a fee to that transaction which will reward the

[49] *See infra* at 17.



miner who wins the leader lottery and is the first to incorporate the transaction in the blockchain.[50]

Relying on these proof-making nodes to write data may seem like a kind of permissioning, and it is true that any particular user who is chosen in the leader lottery can, for that period, decide which new data will and which new data will not be written to the blockchain. Taking Bitcoin for example, it is true that for the duration that a miner wins the leader lottery, she can censor or block any other user from transacting.

There are two factors that make these systems permissionless in spite of the power of miners or proof makers to block or screen write-access: self-interest among competing proof makers, and ignorance of the data that enters the blockchain.

Self-interest. If a user wants to ensure that her transaction will be added to a public blockchain, she can append a fee to the transaction.[51] Miners or proof makers on the network compete with each other for the block rewards that come with winning the leader lottery. Block rewards are comprised of any fees that were appended to transactions as well as any new money being created through programmed inflation. It is with these block rewards that miners can finance the expensive hardware and electricity necessary to perform competitive proof-of-work calculations or justify the costly sacrifice of tokens necessary in making a proof of stake. Blocking transactions will reduce the fee-revenue component of the block reward, leaving censorship-favoring proof makers at a competitive disadvantage. Therefore it goes against the self-interest of proof makers to selectively censor (*i.e.*, permission) the network. Additionally, to the extent that a network is famed for being censorship resistant, *e.g.* Bitcoin,[52] negative publicity from a proof maker's decision to censor transactions may erode faith in the network as a whole. This could cause the market price of the network's tokens to fall, thereby reducing the real value of the proof maker's returns and/or motivating the community to enforce anti-censorship norms by shaming the offending proof maker.

Ignorance. Proof makers may not have very much information about the data they are writing to the chain. In other words, the proof maker may know that a particular transaction is valid (because the digital signatures are valid and the sending address is appropriately funded) but she may have no way of knowing who the real-world sender or recipient in the transaction could be. As we will discuss in the section on privacy,[53] new technologies such as zero-knowledge proofs, could ensure that proof-makers as well as the public can gain effectively no information from the blockchain aside from a proof that all transactions are valid according to the consensus rules of the protocol. In this situation, proof-making or mining become an activity divorced from any sort of off-network or personal decision making,

[50] *See* Nakamoto *supra* note 25.

[51] *Id.*

[52] *See, e.g.*, Rainey Reitman, "Bitcoin – a Step Toward Censorship-Resistant Digital Currency" *EFF Deeplinks Blog* (Jan. 2011) https://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant.

[53] *See infra* at 35.

people simply run machines that always add data to the blockchain if it is valid according to the rules of the protocol and are never in a position to discriminate against users for any other reason.

It's simply not necessary to go into this highly nuanced analysis when it comes to consortium-based consensus mechanisms. By definition, these systems will be permissioned at the write-level because only previously identified participants can participate in the consensus. A choice could then be made by the designers of the system, to make read-access to the results of that consensus public or private.

B. Trust Across Consensus Mechanisms

Early decentralized computing systems, like Bitcoin, are designed for serious uses. These networks custody people's valuables, help them move their money.[54] These networks may soon keep track of their users' identity credentials,[55] and eventually even—in the case of the Internet of Things—help them control their door locks, their baby monitors, their cars, and their homes.[56]

A fundamental design goal of these systems is to decentralize control over the network such that a user will not need to trust a bank-like company's honesty in order to safeguard her money,[57] or trust a technology company in order to safeguard access to her smart home devices.[58] Who or what do you trust to guarantee these systems if not a reputable intermediary, and how does that model of trust change depending on the type of consensus mechanism employed in the system's design? These are the questions addressed in this subsection.

To start, any discussion of trust must deal with three essential subtopics:

- **Software:** Every system described in this testimony is built from software, and the auditability of that software, as well as the nature of the process of writing that software is the first concern we should have when we ask ourselves: can I trust this system?

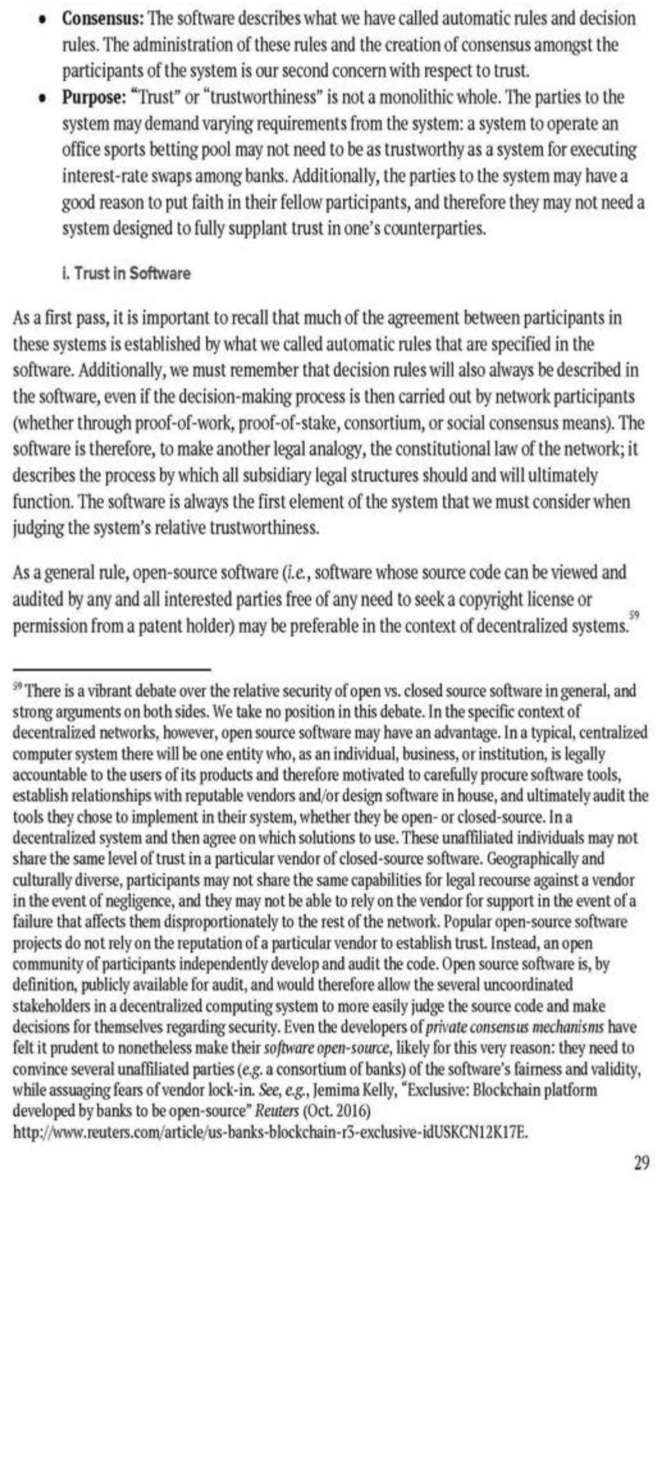
[54] *See infra* at 45. *See also* Nakamoto *supra* note 26.

[55] *See infra* at 51. *See also* Ali *supra* note 5.

[56] *See infra* at 58. *See also* Peter Saint-Andre, "How can blockchains improve the Internet of Things?" *Coin Center* (Oct. 2016) https://coincenter.org/entry/how-can-blockchains-improve-the-internet-of-things.

[57] *See* Nakamoto *supra* note 26 ("What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.").

[58] *See* IBM Institute for Business Value, *Device Democracy: Saving the future of the Internet of Things*, https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF ("The Internet was originally built on trust. In the post-Snowden era, it is evident that trust in the Internet is over. The notion of IoT solutions built as centralized systems with trusted partners is now something of a fantasy. Most solutions today provide the ability for centralized authorities, whether governments, manufacturers or service providers to gain unauthorized access to and control devices by collecting and analyzing user data.").



- **Consensus:** The software describes what we have called automatic rules and decision rules. The administration of these rules and the creation of consensus amongst the participants of the system is our second concern with respect to trust.
- **Purpose:** "Trust" or "trustworthiness" is not a monolithic whole. The parties to the system may demand varying requirements from the system: a system to operate an office sports betting pool may not need to be as trustworthy as a system for executing interest-rate swaps among banks. Additionally, the parties to the system may have a good reason to put faith in their fellow participants, and therefore they may not need a system designed to fully supplant trust in one's counterparties.

i. Trust in Software

As a first pass, it is important to recall that much of the agreement between participants in these systems is established by what we called automatic rules that are specified in the software. Additionally, we must remember that decision rules will also always be described in the software, even if the decision-making process is then carried out by network participants (whether through proof-of-work, proof-of-stake, consortium, or social consensus means). The software is therefore, to make another legal analogy, the constitutional law of the network; it describes the process by which all subsidiary legal structures should and will ultimately function. The software is always the first element of the system that we must consider when judging the system's relative trustworthiness.

As a general rule, open-source software (*i.e.*, software whose source code can be viewed and audited by any and all interested parties free of any need to seek a copyright license or permission from a patent holder) may be preferable in the context of decentralized systems.[59]

[59] There is a vibrant debate over the relative security of open vs. closed source software in general, and strong arguments on both sides. We take no position in this debate. In the specific context of decentralized networks, however, open source software may have an advantage. In a typical, centralized computer system there will be one entity who, as an individual, business, or institution, is legally accountable to the users of its products and therefore motivated to carefully procure software tools, establish relationships with reputable vendors and/or design software in house, and ultimately audit the tools they chose to implement in their system, whether they be open- or closed-source. In a decentralized system and then agree on which solutions to use. These unaffiliated individuals may not share the same level of trust in a particular vendor of closed-source software. Geographically and culturally diverse, participants may not share the same capabilities for legal recourse against a vendor in the event of negligence, and they may not be able to rely on the vendor for support in the event of a failure that affects them disproportionately to the rest of the network. Popular open-source software projects do not rely on the reputation of a particular vendor to establish trust. Instead, an open community of participants independently develop and audit the code. Open source software is, by definition, publicly available for audit, and would therefore allow the several uncoordinated stakeholders in a decentralized computing system to more easily judge the source code and make decisions for themselves regarding security. Even the developers of *private consensus mechanisms* have felt it prudent to nonetheless make their *software open-source*, likely for this very reason: they need to convince several unaffiliated parties (*e.g.* a consortium of banks) of the software's fairness and validity, while assuaging fears of vendor lock-in. *See, e.g.*, Jemima Kelly, "Exclusive: Blockchain platform developed by banks to be open-source" *Reuters* (Oct. 2016) http://www.reuters.com/article/us-banks-blockchain-r3-exclusive-idUSKCN12K17E.

Open-source practices provide an opportunity for developer transparency, an opportunity for a developer or group of developers to put their cards on the table and show with precision what it is they are building. It also subjects that design to an unbounded set of potential security auditors who may detect innocent mistakes as well as malicious backdoors.[60] Without visibility into the software we are putting a good deal of faith in the person selling us that software or advocating for its use. Closed-source software, also referred to as proprietary software, may be superior for various applications (*e.g.*, a word processor or a game), but for decentralized applications that we intend to trust with our money, reputation, identity, or any other valuable agreement between users, close- source software creates real risks. To extend our legal metaphor, a closed-source consensus protocol is not unlike a constitution that no one in the country is allowed to read without seeking permission from the drafter or central government.

To give a real-world example, imagine if someone decided to create an alternative to Bitcoin by copying and modifying the Bitcoin software. What if this person changed the automatic rule that requires all transactions to be funded by prior transactions, to a rule stating that one particular pseudonymous participant would be allowed to send transactions out of thin air. If we are going to use this bizarro-Bitcoin as a shared currency, we would certainly want to know that this change to the software's automatic consensus rules has been made. Our new bizarro-Bitcoin network is now allowing one special user to print money to her heart's content. If we have no way to freely read and audit that code (or to rely on a diverse range of third-party validators to do that audit independent of the software author) then we have no reason to trust the network it creates or the agreements it powers.

ii. Trust in the Consensus

After looking at the software, we next need to judge the trustworthiness of the consensus mechanism implemented by the software. Regardless of what some more fervent advocates of these new technologies may say, no system is truly "trustless." No system relies purely on "math" or "cryptography" to ensure that the agreement reached by the network is in any way just or perfect. Instead, these systems are designed to be *trust minimizing*, designed to rely as little as possible on the honesty of the network's participants, usually by making deceptive or fraudulent participation go against the economic interests of the participants. So, aside from being public or private, we can also discuss how each category of consensus mechanism attempts to minimize trust.

In proof-of-work and proof-of-stake systems, so long as we believe that the participants who together control a simple majority of the total computational power on the network (for proof-of-work) or the staked token value on the network (for proof-of-stake) are behaving honestly, then the network's decision rules will work as intended. The need for trust in the

[60] The idea of security by way of massive public auditing and transparency has come to be called "Linus'Law" and it is commonly expressed as "Many Eyes Make All Bugs Shallow." See Jeff Jones, "Linus's Law aka 'Many Eyes Make All Bugs Shallow'" Microsoft Cyber Trust Blog (Jun. 2006) https://blogs.microsoft.com/cybertrust/2006/06/07/linuss-law-aka-many-eyes-make-all-bugs-shallow/.

network's participants is obviated so long as half of its participants are not united in trying to attack it. If a dishonest party or parties assumes control of a simple majority of the computational power or staking ability on the network, then they can effectively control the outcome of all decision rules, and the results may differ substantially from the expectations of honest participants.

To take Bitcoin as an example, a party with majority control of the network's total computational power could: (1) refuse to put certain transactions into the shared ledger indefinitely, (2) consistently favor her own transactions over others in the speed with which they are recorded in the ledger, and (3) periodically rearrange the ledger's order going back as far in history as she has had the majority of power on the network.[61] She cannot, however, violate the automatic rules on the network: she cannot spend other people's bitcoins, nor can she create more bitcoins than would normally be allowed under the monetary policy rules of the software. By sending messages that violate these automatic rules, she loses compatibility with the network and ceases to take part in the consensus mechanism that enforces decision rules like transaction order.

So in proof-of-work and proof-of-stake systems, we can generally trust that the shared computation is valid and fair so long as we believe it is cost-prohibitive for a malicious actor to amass sufficient computing power or staked tokens to have a majority on the network.

Proof-of-stake systems still lack a robust working prototype. The most notable system, Peercoin, suffered a spate of attacks and reverted to a state where the developers created a whitelist of permissible stakers (effectively a consortium model).[62] Some theorize that a robust proof-of-stake consensus mechanism is an impossible goal, but considering that is beyond the scope of this testimony.[63]

The availability of what is called "forking"[64] adds an additional wrinkle to the question of trust

[61] This is commonly referred to as a 51% attack. The limited ability to do harm and exorbitant cost of the attack, combined with the ease with which an attack would be noticed by the community and resolved with modifications to core software lead many to believe that such attacks should be low on the list of threats to the security and trustworthiness of the Bitcoin network. *See* Gavin Andresen, "Neutralizing a 51% Attack" *GavinTech* (May 2012) http://gavintech.blogspot.com/2012/05/neutralizing-51-attack.html; *see also* Daniel Cawrey, "Are 51% Attacks a Real Threat to Bitcoin?" *Coindesk* (June 2014) http://www.coindesk.com/51-attacks-real-threat-bitcoin/.

[62] Andrew Poelstra, "A Treatise on Altcoins" 14 (Mar. 2015) https://download.wpsoftware.net/bitcoin/alts.pdf.

[63] For a technical analysis of proof-of-stake systems see Poelstra *supra* note 61 at 14.

[64] This use of "fork" comes from the larger world of free and public source software development, particularly the communities developing Linux, the open source and oft-forked operating system that powers many enterprise computing systems. Forking refers to a decision amongst some developers within an open source project to duplicate the code of that project and maintain it separately in order to create some derivative invention. See Benjamin Mako Hill, "To Fork or Not To Fork: Lessons From Ubuntu and Debian" (May 2005) https://mako.cc/writing/to_fork_or_not_to_fork.html ("The act of taking the code for a free software project and bifurcating it to create a new project is called "forking." There have been a number of famous forks in free software history. One of the most famous was the schism that led to the parallel development of two versions of the Emacs text editor: GNU Emacs and XEmacs.

in networks that utilize public consensus mechanisms. If two or more factions of users on the network fail to reach an agreement over what we have called "automatic rules," then the network will divide in two or more parts. They will share a computational history up until this impasse but, from the time that one faction chooses to alter their software's automatic rules onward, they will forge new and distinct futures. This has been the case in several so-called *hard forks* of cryptocurrency networks.[65]

To understand the trust implications of hard forks, we need an example. According to an automatic rule in the Bitcoin consensus mechanism, which we'll call the *supply rule*, there can only ever be 21 million bitcoins.[66] This hard limit in the code forms the basis of Bitcoin's value proposition: you are willing to hold and trade these otherwise made-up tokens for real goods because their supply is known to be finite. With supply fixed, any demand from a community of users will result in a positive price. If we choose to trust Bitcoin's long-term valuation, we'll have to worry about fluctuations in demand affecting the price, but at least we won't need to worry about an increase in supply diluting the value of our holdings with inflation. The effect of the *supply rule* is to Bitcoin's value as the effect of the earth is to the value of gold when it resists gold-mining.

While it has never happened, we could imagine a fork of Bitcoin where part of the network wants to increase the total supply of bitcoins from 21 to 42 million by changing that automatic rule. We'll call the more-bitcoins partisans KeynesCoiners, and the rest of the users we'll call MiltonBitters. As soon as the KeynesCoiners update their software to incorporate a change in the supply rule, transactions and blocks from a KeynesCoin computer are invalid when received by a MiltonBit machine and vice versa. Both sides of the network recognize a common history of bitcoin transactions, but going forward they will have irreconcilable futures. If you

This schism persists to this day.").

[65] The most notorious fork in recent crypto-times is probably the hard fork of Ethereum during the DAO hack in the summer of 2016. In response to a bug in a widely funded smart contract (the DAO), developers offered a change to the core protocol that would effectively unwind the result of that contract on the blockchain and make DAO investors whole. A minority of network participants disagreed with this policy and refused to update their software. The result was a fork of the network and the creation of Ethereum Classic (effectively an alternative version of Ethereum). While the drama generated a good deal of press from those critical of Ethereum or simply interested in these networks, it should be noted that the price of Ethereum two months before (April 18th: $8.44) and two months after the fork (August 18th: $11.06) shows little evidence for an erosion of trust in the network. For more on the Ethereum fork see Joon Ian Wong and Ian Kar, "Everything you need to know about the ethereum hard fork" *Quartz* (July 2016) http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/.

[66] There is no line of code in the Bitcoin reference client that specifically says, "there will only ever be 21 Million bitcoins." Instead, there is language that describes the permissible size of the reward of new bitcoins that miners who mine new blocks can claim in a coinbase transaction. This reward is referred to as a "block subsidy" and it is coded to start at 50 bitcoins per block and decrease by half on a schedule that would result in a final total supply of roughly 21 million total bitcoins at some point in the year 2140. See Bitcoin Core,"main.cpp," https://github.com/bitcoin/bitcoin/blob/master/src/main.cpp, lines 1380-1391 ("Subsidy is cut in half every 210,000 blocks which will occur approximately every 4 years."). See also "Controlled supply," Bitcoin Wiki, https://en.bitcoin.it/wiki/Controlled_supply (last accesed Dec. 2015).

held bitcoins before the fork, you now have bitcoin balances on both networks (because they share a common history before the fork), and you can run KeynesCoin software on one computer while running MiltonBit on another in order to move your bitcoins on either or both sides of the newly forked network.

Does this violate the trust that users placed in the supposedly sacred 21 million limit? It's hard to say. The MiltonBit network remains a working cryptocurrency for users who want to stick with the 21 million limit, and pro-inflation revolutionaries can switch to the KeynesCoin chain. In fact, now users who are indifferent as to a choice between 21 and 42 can choose to wait it out, or to use both, because their bitcoin holdings are in the history of both sides of the fork and will remain on each chain unless they decide to transact using the compatible software of that chain. To use a term from political science, forking facilitates political *exit* rather than *voice*, leaving a community with whom you disagree rather than lobbying for a change to that community's rules.

It's not all rosy, however. When our hypothetical network split in two, the supply curve changed for only one-half of the network but the demand curve for each coin will probably change for both. Some users will want KeynesCoins and dump their MiltonBit holdings on exchange platforms or over-the-counter trades and vice versa. If a sizable chunk of bitcoiners choose team Keynes, then the price of MiltonBits might fall drastically. If the price of the tokens on open exchanges crumbles, so too could the mining power that safeguards the network against attack.

Rational miners will only spend electricity and capital up to the marginal revenue obtained from mining. If the price of the coin with respect to the cost of electricity and hardware declines, miners will probably take their mining machines offline, or if possible, dedicate their efforts to other more lucrative proof-of-work driven cryptocurrencies. If the total mining power on the network is low enough, a bad actor could corner the mining market more easily and attempt to disrupt the consensus system: block transactions at will, reverse transactions throughout the period in which they have control of the majority mining power, etc.

To round up this forking discussion, we can make the following general observation about trust in public consensus-driven networks. These systems do not create absolute trust or absolutely true computation; they merely generate a single source of truth that is trustworthy (A) only amongst participants who choose to remain compatible with their fellow participants and (B) only so long as a majority of those participants are behaving honestly. These systems do not fully obviate the need for "trust," but instead minimize the amount of trust necessary to a presumption that others will continue to run the software you also want to run, and no party will gain sufficient computational resources or stake sufficient wealth to dominate and then manipulate a leader lottery or other decision rules described by that software.

Consortium systems may be similar in that generally they are only trustworthy so long as a majority of identified consortium members are behaving honestly, and will only function if all members continue to run compatible software. However, we must also consider the entity that identifies and then grants credentials to the consortium members. If this identifying member is corrupted, it could potentially shift the balance of power by granting more participatory rights to one or another consortium member than was assumed to be fair and agreed upon by the other members. The sanctity of a lottery or any other decision rule is only upheld by trust in an identifying agent and the safekeeping of identity credentials by participants (rather than by provable sacrifice of resources by participants). As the developers of Monax, a permissioned blockchain platform, explain:

> The security model for permissioned blockchain networks is very similar [to public consensus networks], namely it is the non-predictive distribution of power over block creation among nodes unlikely to collude. Only, in a permissioned blockchain network the barrier to entry, and/or barrier to control, are provided either out of band by a previous or emergent agreement; added to the genesis block of the blockchain network and/or updated over time as different evolutions of the network become necessary. A possible attack vector at this point for overtaking a permissioned blockchain is thieving (or brute forcing) of 2/3rds of the private keys for the validator set."[67]

Additionally, the nature of an identified consortium may make it easier for some subset of the consensus members to find each other and collude to defraud the rest of the network (at least as compared with a network composed of pseudonymous participants with little or no information about their counterparties).

Finally, social consensus mechanisms are also trust-minimized but in a different manner than the other mechanisms. In a social consensus, you must trust some parties on the network, but need not trust all parties. To the extent that a global consensus is composed of some subset of data that the majority of all trusted participants have validated, we may worry that all participants are blindly placing trust in the same parties without careful consideration of how they should choose. If so, these trusted parties may be able to take advantage of this non-discriminating trust from the network at large and collude to defraud the network just as a majority group could do the same in the other mechanisms we've discussed.[68]

iii. Trust for What Purpose?

To round up our discussion of trust, we also need to consider the question: *trust for what purpose?* Decentralized computing systems are potentially (and in some cases already are) useful for a variety of applications: peer-to-peer electronic cash,[69] identity,[70]

[67] Monax, *What is a Permissioned Blockchain Network?* https://monax.io/explainers/permissioned_blockchains/ *last accessed* Dec. 2016.

[68] Within the Ripple protocol this issue is, in theory, tempered because trusted validators will have reputations to uphold, and should any validator prove untrustworthy users will simply select alternative validators to place on their unique node list. Ripple Wiki: Consensus https://wiki.ripple.com/Consensus *last accessed* Dec 2016.

[69] *See infra* at 45.

[70] *See infra* at 51.

machine-to-machine payments in the Internet of Things,[71] recording property rights,[72] settlement of stock trades,[73] the settlement of accounts between large financial institutions,[74] and more.

In some applications where all participants are part of a tight-knit community with a limited goal (like settling accounts between banks for example), placing trust in an identified consortium and the party doing that identification may be entirely reasonable. Indeed, it may even be reasonable for the software that generates the consensus to be closed source as long as the identified participants (if not the larger public) feel satisfied that sufficient and independent audits of that code have been carried out to ensure that it does in fact do what its developers and vendors claim.

For other applications, however, trust in a central party may be sub-optimal. It could afford certain parties more power over our lives than we would ideally want. Public consensus models are by no means trustless, but they do decentralize power amongst a larger and open set of parties meaning that we are less likely to find ourselves (our transactions, our data, whatever we compute on the network) at the mercy of a single powerful institution that could either maliciously defraud us or negligently fail to maintain a secure network. There are three particular use cases of blockchains for which the trust-minimization inherent in a public consensus mechanism may prove critical: electronic cash, identity systems, and the internet of things. We discuss these in the final section. First, however, we need to discuss privacy.

C. Privacy Across Consensus Mechanisms

As we'll discuss in the final section, decentralized computing platforms may come to be the systems we use to safeguard our money, our identity, and our homes. Our daily activities, our credentials, and our transactions represent a wealth of personal data. The choice of consensus model can have repercussions with respect to our privacy. Who will be able to see your transactions if you use Bitcoin? Who will be able to see your comings and goings if you use a smart lock powered by Ethereum? Before we jump into the technical specifics, however, it's important to carefully describe what we mean by privacy, and what sort of privacy protection we would reasonably want or expect from decentralized computing systems.

i. Privacy and Context

Privacy is never absolute. Even a hermit who never speaks to anyone cannot avoid being seen

[71] *See infra* at 58.
[72] *See* Laura Shin, "Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury" *Forbes* (Apr. 2016) http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#e5b6b4265500.
[73] *See* John Detrixhe, "Scotland to Start Own Stock Exchange Using Blockchain Technology" *BloombergTechnology* (Oct. 2016) https://www.bloomberg.com/news/articles/2016-10-27/scotland-to-start-own-stock-exchange-using-blockchain-technology.
[74] *See* Gendal Brown *supra* note 7.

and scrutinized as she goes about her fishing, foraging or any of the other activities necessary to her survival. So rather than thinking about privacy as the mere ability to avoid public exposure or to keep secrets, let's think of it as the ability to control information about ourselves and our activities. This more nuanced concept is best described by Helen Nissenbaum's term *contextual integrity.*[75] Contextual integrity refers to the ability of an individual to control what information is released and what information is kept private depending on the context of a given social interaction.

Compare, for example, the information we'd want released to our dentist in advance of an appointment with the information we'd want released to our spouse in advance of a night out. These interactions have different contexts: medical and commercial vs. romantic and personal. Therefore, we cannot equate privacy with mere data security. Security simply means withholding some secret. Privacy means controlling to whom and in which situations we choose to reveal those secrets.

Whenever I interact with a decentralized system, I generate information that could become public. If the system is to protect my privacy, then ideally it would only share evidence of my interactions with the minimum set of participants necessary to accomplish my goals and expectations in interacting with the system. It should only share information that is relevant and appropriate within the context of the system as the user understands it.

An example makes this clearer: Let's imagine a system for transferring money. Alice gives money to Bob. Who needs to know what about this transaction? Of course, Alice and Bob need to know the amounts involved and who gets what. Bob also needs to know that the money Alice gave him is real and not a forgery, and he also needs to know that Alice truly gave up that money rather than retaining the ability to spend it. Finally, *everyone* who uses this particular sort of money needs to know that in this transaction no new money appeared unexpectedly, because if Alice somehow managed to both send the money as well as keep it for herself, then the supply of all money has grown and *everyone's* money will be worth a little less because of inflation.

Cash solves these problems by allowing the transaction to occur face-to-face between Alice and Bob. Bob can see that Alice has handed him a ten-dollar note. Bob knows he can walk away with the money and Alice won't be able to get it back. If they perform this ritual behind closed doors, no one else learns about the transaction. Cash notes are designed to make counterfeiting difficult, allowing *everyone* to know with some degree of certainty that no new money was created when Alice and Bob transacted.

Cash doesn't work online because a digital image of a ten-dollar note can be endlessly copied at effectively zero cost. Various solutions for moving money electronically have been developed but, of course, they vary in their ability to respect the privacy of the parties as

[75] Nissenbaum, Helen. "Privacy as contextual integrity." Wash. L. Rev. 79 (2004): 119. *Available at:* http://www.kentlaw.edu/faculty/rwarner/classes/internetlaw/2011/materials/nissenbaum_norms.pdf.

compared with cash.

Alice and Bob can use a bank or several banks in order to account for an electronic movement of money between them. Now Alice and Bob know what they need to know, but the bank also knows about the transaction. If the bank is hacked, the records of the transaction may become public knowledge. Despite having relatively little information to go on, *everyone* must be satisfied that the banks are keeping good records and that they are faithfully serving their role as lenders to maintain the relative scarcity and therefore price of the currency.

Bitcoin is a public consensus-driven peer-to-peer network that creates electronic cash for remote transactions without intermediaries like banks. Bitcoin provides Alice and Bob with the transactional information they need because they can (A) generate and agree on pseudonyms for each other, (B) view a global shared ledger that lists bitcoin balances for all pseudonyms, and (C) only spend balances on that ledger if they have a cryptographic key that matches the pseudonym. Bob knows that Alice has given up the funds because they've moved on the ledger to a pseudonym that only he controls. *Everyone* knows that no new money was created because they can see the transaction moved balances between two pseudonyms but did not create any new bitcoins. *Everyone* could also know the specifics of Alice's or Bob's transactions if the pseudonym(s) used by Alice or Bob can be linked to their name publicly.

Thus we see how three different system architectures (cash, electronic banking, and Bitcoin) all afford the relevant parties to the transaction varying levels of access to and control over the information created by, and necessary for, transacting.

ii. Privacy versus Transparency in Consensus

As we defined it, consensus is an agreement over (1) some set of data, (2) modifications to or computations with that data, and (3) the rules that govern that data storage and computation. An essential feature of these systems is that much of the activities of the participants will be fully transparent and verifiable to all participants in the consensus: the history of the data over which we are forming consensus is auditable and my modifications and computations with that shared data will be transparent so that my actions can be verified. It would be impossible for a network to ensure that the agreed upon rules for data storage and computation are being honored without some level of transparency.

To use Bitcoin as an example, if the full history of bitcoin transactions between users is not transparent, then I have no way of knowing whether a specific user purporting to send me five bitcoins has ever, herself, received or mined those five bitcoins. Similarly, if the transaction from this user to me is not incorporated in the ledger, no future recipient of the funds I've just been sent can be assured that I'm good for the money.

Bitcoin is able to have this level of transparency but still offer some privacy to its users because all of the entities transacting or mining bitcoin on the network are represented by pseudonyms. Specifically, to use Bitcoin I will have my Bitcoin software generate one or more public-private keypairs. The private key is the secret I need to have in order to sign for valid transactions, and the public key is the address or account to which people can send me bitcoins. The public key is a pseudonym. My name may be Peter, but when I transact on the network other machines and users will recognize and address me only by a random string of text:

> 17kdugRB1fdvqFC1BHkBwjZWm2wbt982AH

The problem with this approach is that if anyone learns that I'm the real person behind 17kdug... then they can look up my full transaction history with that address. One solution has been to use several addresses and never reuse an old address. So everytime I ask to be paid, my Bitcoin software will create a new address for me to share with the payor,[76] and everytime I send bitcoin from an address, the remainder or "change" from the transaction is sent to a brand new address. Even with these procedures in place, however, my several addresses could still be linked and identified with forensic tools. For example, if I have two bitcoins each in three different addresses, and I want to pay someone five bitcoins, I will need to use all three of my addresses in order to fund the transaction. With all three of these addresses listed as inputs to the transaction, a nosey person looking at the blockchain can easily assume with some certainty that those three addresses were all one person, me. If any of those addresses have been previously marked as belonging to me, then we're back at the initial problem: my full transaction history is potentially public information.

The same privacy problem is generalizable to any sort of decentralized computing platform powered by the consensus mechanisms we have so far discussed. The need for transparency and verifiability may conflict with our desire for privacy as we use these systems. As we'll see there are two general approaches to resolving or ameliorating this conflict: *perimeter security* and a variety of new techniques, which we can call *data minimization*.

iii. Perimeter Security versus Data Minimization and Selective Disclosure

Faced with an essential trade-off wherein verifiability requires transparency but privacy requires that user-data remain opaque, there are essentially two design options:

1. **Perimeter Security:** Leave all data relevant to the consensus transparent but restrict the set of parties who verify that data to a local and private group of verifiers with whom you are comfortable sharing otherwise private data.
2. **Data Minimization:** Develop tools to only reveal data essential to group consensus if it is absolutely necessary to verification and allow the group of verifiers to be open and global.

Perimeter security follows an older approach in network security generally: *if there are things to be kept secret, we build a secure perimeter, restrict the flow of sensitive information to within*

[76] This is not as inconvenient as it may seem. The wallet software that I use should keep track of all of these addresses and keep the associated private keys secured in a single file (if I'm securing my own bitcoin) or else a company can keep track of this data on my behalf. Either way, when I transact I don't need to worry about a number of addresses and keys, I just spend bitcoins from my wallet.

that perimeter, only allow authorized parties into that perimeter, and carefully monitor for and prevent breaches.[77]

Data minimization takes an alternative approach: *we will not rely on a secure perimeter, all information in the system can be presumed to be global and available, but the only information ever put into to the system is the minimum amount of information necessary to accomplish the goal.*[78]

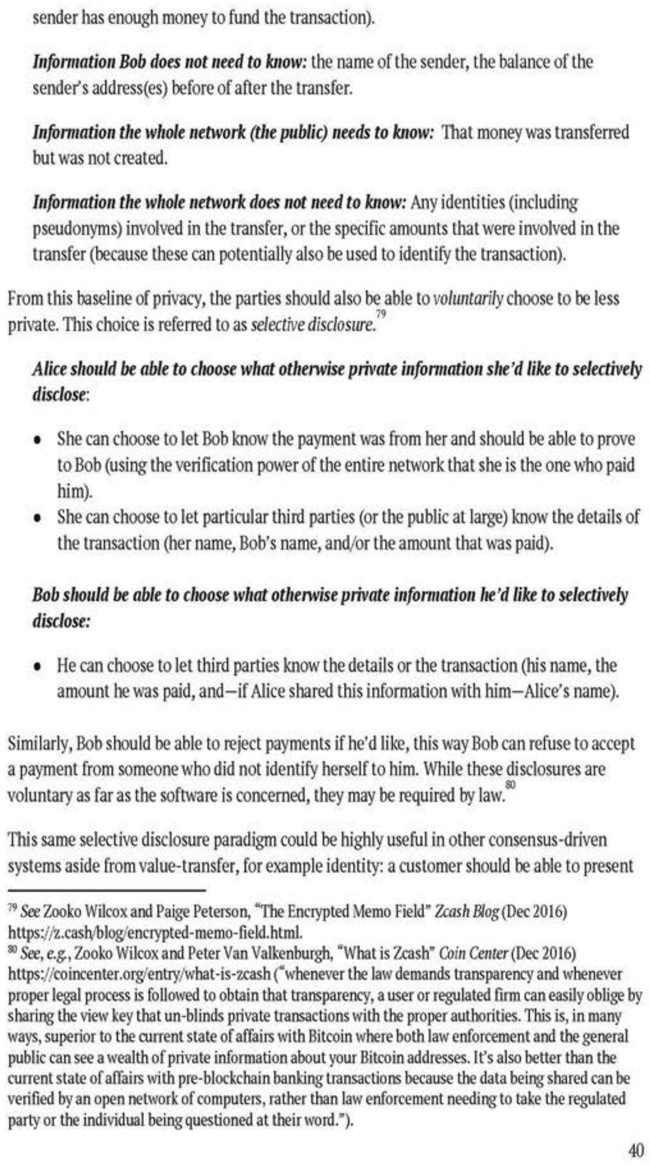
Again, an example will make this distinction clearer. Alice wants to send money to Bob, but wants privacy. A money transmission system with perimeter security would look rather like existing mobile payment applications like PayPal or Venmo. Alice and Bob share the full private details of their transactions with a single verifier, *e.g.* PayPal. PayPal allows Bob to know that Alice has a sufficient balance to send the money, ensures non-repudiation, and by balancing its books gives the public the assurance that no new money was created out of thin air (it was only transferred). As long as PayPal maintains a secure perimeter, the details of these transactions remain private. The downside of this solution is two-fold: (1) we now cannot rely on the larger public to verify the details of the transaction, we must trust the party or group that is within the perimeter (*e.g.*, Paypal), and (2) if the perimeter is ever breached, then all of this data could become public.

A money transmission system employing data minimization instead of a secure perimeter model would look rather like an improved version of Bitcoin. Recall that within Bitcoin, all details of the transactions are public but they are pseudonymous. We have previously discussed how this pseudonymity can be weak and result in the public revelation of an individual user's full transaction history. A system like Bitcoin with more robust data minimization would limit the public data to information that is relevant to consensus and allow the users to choose what additional information they would like to reveal about their specific transaction. Here's what that could look like:

> ***Information Alice needs to know:*** An address where she can pay Bob, confirmation that Bob got paid (in case he tries to claim he didn't).
>
> ***Information Alice does not need to know:*** the balance of Bob's address(es) before or after the transfer.
>
> ***Information Bob needs to know:*** That he's been paid, and that the payment is genuine (the

[77] *See* Lenny Zeltser, Karen Kent, *et al.* "Perimeter Security Fundamentals" *Inside Network Perimeter Security* (Apr. 2005) *chapter available at* http://www.informit.com/articles/article.aspx?p=376256.

[78] *See generally* Peter Schaar, "Privacy by Design" 3 *Identity in the Information Society* 2 (Aug. 2010) *available at* http://link.springer.com/article/10.1007/s12394-010-0055-x/fulltext.html discussing the concept of data minimization within the context of Privacy by Design, *i.e.* "The idea of incorporating technological data protection" into the overall design of an application or computer system, "instead of having to come up with laborious and time-consuming 'patches' later on. ... Privacy by Design goes beyond maintaining security. Privacy by Design includes the idea that systems should be designed and constructed in a way to avoid or minimize the amount of personal data processed. Key elements of data minimization are the separation of personal identifiers and content data, the use of pseudonyms and the anonymization or deletion of personal data as early as possible."



sender has enough money to fund the transaction).

> ***Information Bob does not need to know:*** the name of the sender, the balance of the sender's address(es) before of after the transfer.
>
> ***Information the whole network (the public) needs to know:*** That money was transferred but was not created.
>
> ***Information the whole network does not need to know:*** Any identities (including pseudonyms) involved in the transfer, or the specific amounts that were involved in the transfer (because these can potentially also be used to identify the transaction).

From this baseline of privacy, the parties should also be able to *voluntarily* choose to be less private. This choice is referred to as *selective disclosure*.[79]

Alice should be able to choose what otherwise private information she'd like to selectively disclose:

- She can choose to let Bob know the payment was from her and should be able to prove to Bob (using the verification power of the entire network that she is the one who paid him).
- She can choose to let particular third parties (or the public at large) know the details of the transaction (her name, Bob's name, and/or the amount that was paid).

Bob should be able to choose what otherwise private information he'd like to selectively disclose:

- He can choose to let third parties know the details or the transaction (his name, the amount he was paid, and—if Alice shared this information with him—Alice's name).

Similarly, Bob should be able to reject payments if he'd like, this way Bob can refuse to accept a payment from someone who did not identify herself to him. While these disclosures are voluntary as far as the software is concerned, they may be required by law.[80]

This same selective disclosure paradigm could be highly useful in other consensus-driven systems aside from value-transfer, for example identity: a customer should be able to present

[79] *See* Zooko Wilcox and Paige Peterson, "The Encrypted Memo Field" *Zcash Blog* (Dec 2016) https://z.cash/blog/encrypted-memo-field.html.

[80] *See, e.g.*, Zooko Wilcox and Peter Van Valkenburgh, "What is Zcash" *Coin Center* (Dec 2016) https://coincenter.org/entry/what-is-zcash ("whenever the law demands transparency and whenever proper legal process is followed to obtain that transparency, a user or regulated firm can easily oblige by sharing the view key that un-blinds private transactions with the proper authorities. This is, in many ways, superior to the current state of affairs with Bitcoin where both law enforcement and the general public can see a wealth of private information about your Bitcoin addresses. It's also better than the current state of affairs with pre-blockchain banking transactions because the data being shared can be verified by an open network of computers, rather than law enforcement needing to take the regulated party or the individual being questioned at their word.").

a bartender with an attestation token that proves that an attestor (*e.g.*, the Department of Motor Vehicles) has verified that she's old enough to legally drink, but that token and the decentralized computing system that powers it should not inadvertently disclose her name, address, or anything else about her to the bartender unless she wants to reveal that information.[81]

This architecture has significant advantages over perimeter security. Unlike perimeter security, the choice of remaining private does not come at the cost of trusting a party or a group within a secure perimeter. The validity of the transfer, the fact that no new money was created, and that the transfer cannot be reversed, can all be public information guaranteed by an open set of validators rather than be facts we need to trust a private set of validators to be honest about. Also, with data minimization and selective disclosure there is no central perimeter to be hacked. It's possible that the credentials I use to choose my level of selective disclosure could one day be hacked, and the hacker could reveal all of my transaction records, but there is no central perimeter that, if hacked, would reveal *all private transactions from all users* of the system. The negligence of one user, employee, or vendor partner (failure to set a strong password, willingness to open strange attachments in phishing emails, etc.) does not automatically jeopardize the entire system.[82]

iv. Perimeters or Minimization Techniques in Consensus Mechanism Design

It has been suggested that public consensus mechanisms (*i.e.*, proof-of-work, proof-of-stake, and social consensus) are not suitable for enterprise or financial sector applications because they are not sufficiently private.[83] It is true that Bitcoin presents us with an example of this weakness: pseudonyms are too easily identified and transaction histories of users are too vulnerable to public scrutiny. However, faced with this dilemma, there are a variety of solutions. The commonly cited solution is to build only private, consortium consensus-driven

[81] David Birch has worked diligently to articulate this notion of data minimization and transactional identity. As Birch frames it: "What is needed to enable transactions is not identity per se but the associated entitlements." Not, "I am John Doe" but instead "I am old enough to order this beer." Birch calls this form of identification "pseudonyms with credentials." David Birch, Identity is the New Money (2014).

[82] Take for example the 2015 Target breach. At Target, consumer credit card credentials were stored on an internal server, but hackers did not initially infiltrate this server. Instead, they targeted a vulnerable server controlled by a heating and cooling company that Target used as a facilities services vendor. By granting some network access to this vendor, Target unknowingly and unintentionally extended the network of trust to which its customers belonged. Once the heating and cooling company was compromised, so was Target and so were all of their customers. With enough new and variable links in a chain, one is likely to be weak enough to unravel the whole. *See* Brian Krebs, "Target Hackers Broke in Via HVAC Company," *KrebsonSecurity* (Feb. 2015) http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

[83] *See*, *e.g.*, ESMA, Discussion Paper: The Distributed Ledger Technology Applied to Securities Markets (Feb. 6, 2016) https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf ("We understand that the DLT [distributed ledger technology] that is likely to be applied to securities markets would be 'permission-based' in contrast to the 'permissionless' system that was originally designed for virtual currencies, *e.g.*, Bitcoins, for a number of reasons, including efficiency, security and privacy purposes.")

networks for these use-cases. The only privacy gain inherent to this approach is the creation of perimeter security. For example, the banking technology consortium R3 has described its Corda decentralized ledger product as follows:

> "The foundational object in our concept is a state object, which is a digital document which records the existence, content and current state of an agreement between two or more parties. It is intended to be shared only with those who have a legitimate reason to see it."[84]

Privacy is thus ensured by sharing the "state object" only with one's trusted counterparties, with those "who have a legitimate reason to see it." The agreement is made private by placing it behind a secure perimeter, not necessarily by limiting the contents of the agreement to data relevant to consensus over that agreement. If any of the "legitimate" parties are compromised, the contents of the agreement could become public. In this sense the consortium model on its own does little to change the state of information security beyond what we see from existing centralized financial intermediaries. Indeed, it may be on balance a more vulnerable system because the secure perimeter now includes employees at other firms. Additionally, if the entire contents of the agreement are private to the relevant parties, independent validation of the data cannot occur in a fully trust-minimized manner (*i.e.*, from an open and global network of impartial transaction validators); one only gets validation from the set of parties permitted by the consortium to enter the secure perimeter.

To R3's credit, it is investigating various other approaches to better enhance privacy as described in their near- to mid-term roadmap:

> Privacy enhancements using technology such as address randomization, zero-knowledge proofs.[85]

These are approaches that apply equally well in consortium and public consensus-driven systems. Significantly, these technologies have been primarily pioneered in the Bitcoin and related cryptocurrency communities.

Address randomization is effectively the attempt to create more robust pseudonyms that fail to yield to forensic identification techniques. Most research into the development of these techniques is occurring in the Bitcoin space where, without robust address randomization, privacy is fairly poor as previously described. Notable pioneering advances in this approach are the CoinJoin[86] and Coin Shuffle[87] protocols, which create decentralized communications

[84] Corda Introductory Whitepaper (Aug. 24, 2016) http://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda2fdebbd1acc9c0309b2/1472045822585/corda-introductory-whitepaper-final.pdf.

[85] *Id.*

[86] Blockchain.info, SharedCoin and other CoinJoin implementations: Uses and Limitations (June 10, 2014) https://blog.blockchain.com/2014/06/10/sharedcoin-and-other-coinjoin-implementations-uses-and-limitations/.

[87] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate, CoinShuffle: Practical Decentralized

channels to facilitate the shuffling of bitcoins between several addresses in a manner that makes it difficult to link a set of addresses to one particular user. Additionally, changes to the Bitcoin core protocol have been researched and proposed that would obscure the value of each transaction as it appears in the blockchain, a project referred to as Confidential Transactions.[88] Simultaneously, some security researchers have proposed that key concepts from the Confidential Transactions and CoinJoin protocols, could be combined and used to obscure both the value and the participants to a transaction. This new research has been referred to, whimsically, as Mimblewimble (from the Harry Potter books) and it is now being developed into a standalone cryptocurrency called Grin.[89]

Separately, Zero-knowledge proofs are a cryptographic tool for proving some important fact (*e.g.*, this transaction is valid, these bitcoins have never been spent by this sender before), without revealing any other information aside from the proof.[90] Integrating zero-knowledge proofs into a public consensus blockchain could potentially allow a decentralized open set of transaction validators to prove that all recent transactions have been appropriately funded, signed, and not double-spent, without revealing any additional information about who sent how much to whom. The Zcash Electronic Coin Company has been pioneering these technologies in the form of Zcash, a public consensus (proof-of-work) driven digital currency network. Not only is Zcash testing the viability of a truly data-minimized approach to privacy and consensus, the protocol also allows users to selectively disclose information about their transactions to whomever they choose.

> Zcash transactions automatically hide the sender, recipient and value of all transactions on the blockchain. Only those with the correct view key can see the contents. Users have complete control and can opt-in to provide others with their view key at their discretion.[91]

Still another cryptographic tool that can be utilized to provide privacy alongside reliable verification of data on a public blockchain is a ring signature. Briefly, these signature schemes can be employed to prove that one of several members of a group authoritatively signed a message without revealing which member of the group actually did the signing. Ring signatures are already employed by the cryptocurrency Monero to protect user privacy.[92]

These systems are in many ways be ideal: Trust in the scarcity of the underlying tokens and the non-reputability of transactions is generated by an open set of impartial validators (rather

Coin Mixing for Bitcoin https://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/coinshuffle.pdf

[88] "The Elements Project Confidential Transactions," https://www.elementsproject.org/elements/confidential-transactions/

[89] "Grin, the Tech," https://grin-tech.org/

[90] *See* Wilcox *supra* note 79.

[91] Giulio Prisco, Zcash Creator on the Upcoming Zcash Launch, Privacy and the Unfinished Internet Revolution (Aug. 30, 2016) https://bitcoinmagazine.com/articles/zcash-creator-on-the-upcoming-zcash-launch-privacy-and-the-unfinished-internet-revolution-1472568389.

[92] "Ring Signature," *Moneropedia*, https://getmonero.org/resources/moneropedia/ringsignatures.html.

than a consortium of identified but potentially corrupt or infiltrated parties). Privacy is guaranteed by neglecting to share any information about transactions with these validators except for the minimized amount of information necessary to prove scarcity and non-repudiation. Additionally, selective disclosure ensures that counterparties and third parties can be given visibility into the details of any particular transaction whenever the initiator wishes to be transparent or is compelled to be transparent by regulation or investigation.

IV. Use Cases in which Public Consensus is Critical

There are many use cases or applications that can be created and deployed equally well on public or private blockchain networks. There are, however, certain use cases that can only achieve their full potential if they use a public and permissionless blockchain network. These use cases for which public consensus is critical, not coincidentally, also happen to be at the fundamental level of information systems: identity, security, and payments.

The most obvious use case in which public consensus is critical is in building *general purpose* decentralized computing networks—the decentralized computing platforms discussed at the start of this testimony. Just as the Internet has become a public platform for the proliferation of innumerable useful applications dealing primarily with communication of information, so too could networks like Bitcoin, Ethereum, Zcash, Monero, or Grin become platforms for innumerable applications dealing primarily with recordkeeping, exchange, and governance. The principle advantage of using public consensus mechanisms to form the basis of these platforms is the dynamism and diversity inherent in an open ecosystem of application developers, where developers need not seek permission to tinker with, create, and test a new idea.

But speaking abstractly of a variety of applications that will presumably emerge in a non-permissioned environment is not particularly satisfying. So for the remainder of this testimony we will discuss three specific, promising use cases that would particularly benefit from being built on top of public platforms.

The three use cases we will highlight can all be thought of as *applications*, a word we have thus far thrown about haphazardly without definition. By applications we mean *human jobs or problems that benefit from computing.* At the start of each subsection we will specify the specific human job or problem under discussion, and then go on to explain why that application would benefit from being built on top of a public consensus mechanism rather than a private and permissioned system.

A public consensus mechanism decentralizes trust, spreading out power on the network across a larger array of participants. In general, decentralization helps ensure **user sovereignty**, **interoperability**, **longevity**, **fidelity**, **availability**, **privacy**, and **political neutrality**. These attributes will be explained in the context of each application, and a discussion of public and private consensus mechanisms for that application will follow.

Speaking generally, however, and abstracting away some technical nuance, public consensus mechanism are critical in use cases where any of these attributes are desirable because only by including the user's device or an unbounded set of disinterested proxies for that user's interests in the consensus mechanism (by designing that mechanism such that *anyone* can participate and not just an empowered few) can the user free themselves from reliance on a single centralized counterparty to guarantee their privacy, the longevity of the network, the fidelity of the data in the blockchain, etc.

Again, public consensus mechanisms and the scarce tokens (like bitcoin or ether) that incentivize participation in the consensus, are not merely an artifact of the political biases of the initial creators of these technologies, they are also essential to the well-functioning of any system that desires user empowerment. So in the cases discussed below—electronic cash, identity, and the Internet of Things—we will explain why individual user empowerment is essential to the use case, and therefore, why public consensus mechanisms like proof-of-work or proof-of-stake are essential to building the infrastructure that powers those consumer or business applications.

A. Electronic Cash

Bitcoin was the original blockchain and public consensus mechanism, and the white paper that first described the invention clearly describes the application it promised: "A purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution."[95] Note that the design is more specific than often reported. Bitcoin was not designed to be a settlement tool for financial institutions, a lending or borrowing tool, a register for financial instruments, or a repository for any other sort of data. Bitcoin was designed to do one thing: enable cash-like (as in similar to paying with paper notes) transactions on the Internet.

i. What is Cash? Why is it Difficult Online?

Cash is a settlement tool, a very simple one that we tend to take for granted. Say I owe you $20 because you are a restaurateur who's just provided me with an excellent lunch. I have a debt that I can now settle very easily if I have cash: I hand you a $20 bill; done.

The peculiar utility of cash is derived from it being a fungible bearer instrument. A *bearer instrument* simply means that whoever holds the instrument is entitled to the rights described in the instrument.[94] The rights described by a $20 note were, historically, redemption by a bank or government of an equal amount in "real money" like gold coinage. The transition to fiat money altered that right subtly to redemption of any equally sized debt, public or private. In either case the possessor of the right is whoever holds the $20 note. *Fungible* means that any particular $20 note carries the same rights as any other $20 note (indeed two $10 notes

[95] *See* Nakamoto *supra* note 26.

[94] *See* William E Britton, "Transfers and Negotiations Under the Negotiable Instruments Law and Article 3 of the Uniform Commercial Code" 32 Tex. L. Rev. 153 (1953-1954).

together carries the same rights as well).

Fungible bearer instruments reduce transaction costs within any economic exchange.[95] In the midst of any given transaction, say paying the tab at a restaurant, neither party needs to pause and inquire as to the provenance of the note, whether it rightfully belonged to the buyer according to some authoritative registry of notes, or whether this particular note is blacklisted by virtue of being used previously in a crime or pledged as collateral in some ill-fated loan. Instead, the buyer presents the note, it looks like any other note, and would—as any other note—buy as much lunch. The transaction happens fluidly and without delay because the parties do not need to engage in fact finding or deep contemplation about the medium of exchange presented. Transaction costs are minimized. This particular reduction in transaction costs has long been understood as essential to a well-functioning economy. Take, for example, a report of the policy arguments made in a formative Scottish case on the subject of bank notes and fungibility in 1749:

> Policy issues, as might be expected, were highly prominent in Lord Strichen's Report. Trade, it was argued for the Banks, rested on the free circulation of money, and free circulation rested in turn on the reliability of notes and coins. If Crawfurd [the plaintiff, a previous holder of a bank note, and from whom the note in question was stolen] was able to vindicate the banknote, no merchant could risk taking money in payment 'without being informed of the whole History of it from the Time that it first issued out of the Bank or the Mint till it came to his Hand, which is so apparently absurd, that it seems hardly to merit a Consideration'. And as banknotes would thus be rendered 'absolutely useless', this would 'in a great Measure deprive the Nation of the Benefit of the Banks, which could hardly subsist without the Circulation of their Notes'. It was in vain for [opposing counsel] to object that, just as people continue to buy goods despite the (slight) risk that they might be stolen and subject to vindication, so they would continue to accept money if the risks were the same. If money could be vindicated, counsel for the Bank of Scotland concluded, 'no Man could be sure, that one Shilling in his pocket was his own, and ... Banks might shut their doors.'[96]

Crawfurd lost his case and the fungibility of cash was guaranteed by the courts in Scotland. Similar decisions followed in other jurisdictions, and the fungible paper currency we know and rely on to this day was assured.

Compared with cash, pre-Bitcoin online transactions had relatively high transaction costs. This is because all electronic instruments are, effectively, registered instruments rather than bearer instruments. A *registered instrument* means that the rights associated with the

[95] *See generally,* David Fox, *Property Rights in Money*, §§ 2.11–2.20 (2008).

[96] *See* Kenneth Reid "Banknotes and Their Vindication in Eighteenth-Century Scotland" *University of Edinburgh, School of Law, Working Papers* (Nov. 2013) http://www.research.ed.ac.uk/portal/files/13523302/Reid_Banknotes.pdf. *quoting* Lord Strichen, Reporter, *Minutes, the Governor and Directors of the Bank of Scotland against the Governors and Directors of the Royal Bank and others* (21 February 1749).

instrument adhere only to the person whose name appears in some authoritative register, the current bearer of a particular certificate or note related to that instrument is irrelevant.

The reason why electronic instruments must be registered is straightforward. Digital files, like Microsoft Word documents or MP3 music files, can be costlessly duplicated. While the reproduction of a music CD will necessarily entail the costs inherent in the production of another physical thing, digital music files can be replicated with almost no effort or expense. If the bearer of a particular file is entitled to rights described in that file, and any person can almost costlessly copy the file again and again, then it is trivial to effectively manufacture more rights. A $10 file on my computer, if copied over and over can become a billion dollars. To address this, banks or other intermediaries will keep a centralized record (*i.e.*, a registry or ledger) of who has which rights to which electronic funds. If I claim to pay an online retailer, the retailer's computer effectively calls up my bank to make sure I have the money I say I do.

These registered instruments require mutual trust in the ledger keeper. If I'd like to pay you electronically, we'd both need to have an account at the same bank or else use an additional intermediary, like a correspondent bank or a credit card company, who can be a trusted go-between for our particular banks.

All of these intermediaries generate transaction costs. The magnitude of these costs will depend on the efficiency of the intermediaries, and the number of intermediaries necessary to build a trustworthy bridge between myself and the person I'm paying. Each may take a fee; each will take their time to process the transaction.

There are also hidden costs in these systems: chargebacks, and transactions forgone. Credit cards, for example, may appear to offer near instant transactions, but in reality the credit card company only *authorizes* future payment between the banks of the parties. If when that future payment goes to be settled (and even after the settlement), it turns out that the card has been reported stolen, the merchant receiving the payment may suffer a chargeback (*i.e.*, they will not receive the sum they were promised and they will bear the loss of the real goods they gave in exchange).[97] Additionally, when transaction costs are high, small-value transactions become cost-inefficient and people will simply avoid making them. This is the case with microtransactions to pay for or meter low-value digital goods (*e.g.*, a minute of Wi-Fi at the airport, the ability to read just one article on a pay-walled website).[98] Another substantial hidden cost is the unavailability of electronic payment to those who cannot obtain a banking relationship. Several billion people across the world do not have banking relationships, often through no fault of their own.[99] Banks will frequently deem a prospective customer's personal

[97] When goods are purchased using stolen credit cards, the merchant is generally left taking the loss. The Bureau of Justice Statistics estimates that these losses cost Americans over $24.7 billion in 2012 alone. That's 10 Billion more in losses than all other property crimes combine." *See* Bureau of Justice Statistics, Data Collection: National Crime Victimization Survey (NCVS) (2012) *available a*t http://www.bjs.gov/index.cfm?ty=dcdetail&iid=245.

[98] *See* Chris Smith, "What are Micropayments and How does Bitcoin Enable them?" *Coin Center* (June 2015) http://coincenter.org/entry/what-are-micropayments-and-how-does-bitcoin-enable-them

[99] Asli Demirguc-Kunt, Leora Klapper. Dorothe Singer, Peter Van Oudheusden, " The Global Findex

characteristics or the country where they reside as too indicative of risk for them to be profitable customers.[100] Women and other vulnerable groups are disproportionately affected by bank de-risking.[101] For these people, online transactions are simply not an option and the full global costs of these transactions-forgone goes uncounted.

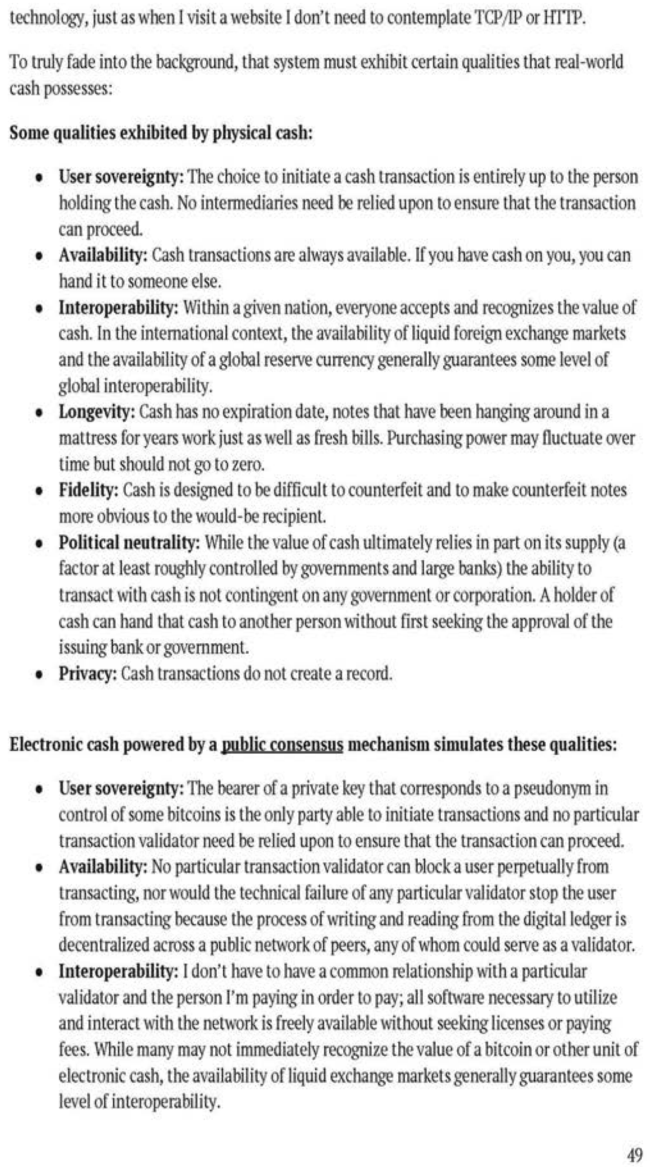
ii. Why Public Consensus is Critical for Cash

In a metaphysical sense, even paper bearer instruments exist on a "register" of sorts, but that register is global, decentralized, and easily made transparent. The register is the world of physical possession. Reading from the register looks like this: *whose hands or pockets hold which instruments?* And writing to it looks like this: *accept the note from the person who is handing it to you.* It is similar with bitcoin, but instead of hands and pockets and the physical world we have software and a global network. Bitcoin's key innovation was to *simulate* a bearer instrument digitally by using networked software to fully automate and decentralize the registry of instruments, such that the "registry" component of the instrument effectively fades into the background. My bitcoins are still described on a register and that's why I can't duplicate them willy-nilly, but the register is merely an unowned, shared, and ubiquitous feature of networked computers (just like the Internet is an unowned, shared, and ubiquitous communications feature for most computers today—and just like the ability to exchange paper notes or stuff them into wallets or safes is a ubiquitous feature of the physical world). When I transact with bitcoins I don't need to consider the blockchain or peer-to-peer networking

Database 2014 Measuring Financial Inclusion around the World" *World Bank Policy Research Working Paper* 7255 (April 2015) *available at* http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf#page=3.

[100] *See* Tracey Durner and Liat Shetret, "Understanding Bank De-Risking and its Effects on Financial Inclusion" *Oxfam Research Report* (Nov. 2015) *available at* https://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/rr-bank-de-risking-181115-en_0.pdf. ("As financial institutions re-calculate risk appetites and decide to exit relationships, they directly and negatively affect these sectors and the populations they serve. For example, in August 2014, Westpac Banking Corp. followed other major Australian and UK banks and announced the closure of numerous money transfer operators' accounts over concerns about AML/CFT and rising compliance costs. This followed the precedent set in the wake of Barclays' May 2013 decision to close money transmitter accounts and the subsequent temporary injunction filed by Dahabshiil, one of the largest Somali remittance companies in the UK. The closure of these bank accounts not only threatens these businesses but also jeopardizes the vital flow of remittances to Somalia from diaspora populations, which constitute an estimated 25 to 45 percent of the country's GDP and serve as a key source of income for more than 40 percent of its vulnerable population.

[101] *Id.* at 6 ("For example, in developing countries, 46 percent of men have a bank account, compared to 36 percent of women. Immigrants are another heavily affected population: factoring out socioeconomic and demographic considerations, immigrants are six percent less likely to have a checking account and eight percent less likely to have a savings account in the US than their American-born counterparts. Without formal bank accounts, these underserved populations commonly rely on the remittance sector to send money to their families back home, and women have increasingly emerged as a key sending demographic. Although they remit about the same amount as men, women are shown to remit higher percentages of their income, more frequently, and for longer durations than their male counterparts. Reductions in the remittance sectors due to MSB account closures stand to further isolate these communities from the global financial system, exacerbating existing financial inclusion challenges.").



technology, just as when I visit a website I don't need to contemplate TCP/IP or HTTP.

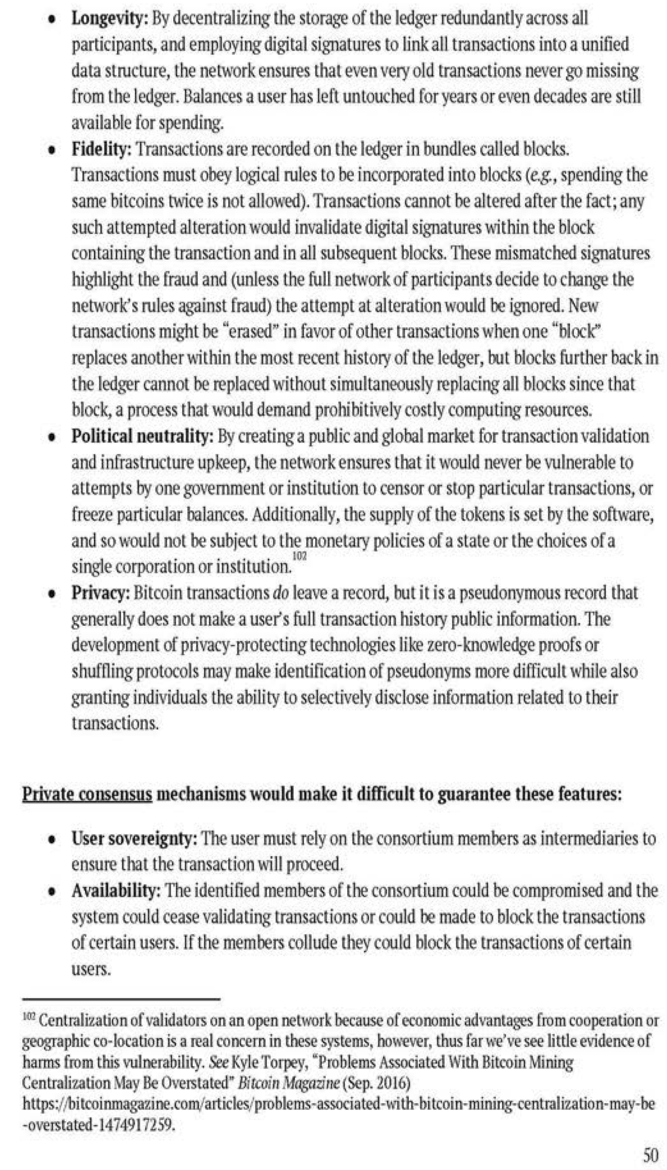
To truly fade into the background, that system must exhibit certain qualities that real-world cash possesses:

Some qualities exhibited by physical cash:

- **User sovereignty:** The choice to initiate a cash transaction is entirely up to the person holding the cash. No intermediaries need be relied upon to ensure that the transaction can proceed.
- **Availability:** Cash transactions are always available. If you have cash on you, you can hand it to someone else.
- **Interoperability:** Within a given nation, everyone accepts and recognizes the value of cash. In the international context, the availability of liquid foreign exchange markets and the availability of a global reserve currency generally guarantees some level of global interoperability.
- **Longevity:** Cash has no expiration date, notes that have been hanging around in a mattress for years work just as well as fresh bills. Purchasing power may fluctuate over time but should not go to zero.
- **Fidelity:** Cash is designed to be difficult to counterfeit and to make counterfeit notes more obvious to the would-be recipient.
- **Political neutrality:** While the value of cash ultimately relies in part on its supply (a factor at least roughly controlled by governments and large banks) the ability to transact with cash is not contingent on any government or corporation. A holder of cash can hand that cash to another person without first seeking the approval of the issuing bank or government.
- **Privacy:** Cash transactions do not create a record.

Electronic cash powered by a public consensus mechanism simulates these qualities:

- **User sovereignty:** The bearer of a private key that corresponds to a pseudonym in control of some bitcoins is the only party able to initiate transactions and no particular transaction validator need be relied upon to ensure that the transaction can proceed.
- **Availability:** No particular transaction validator can block a user perpetually from transacting, nor would the technical failure of any particular validator stop the user from transacting because the process of writing and reading from the digital ledger is decentralized across a public network of peers, any of whom could serve as a validator.
- **Interoperability:** I don't have to have a common relationship with a particular validator and the person I'm paying in order to pay; all software necessary to utilize and interact with the network is freely available without seeking licenses or paying fees. While many may not immediately recognize the value of a bitcoin or other unit of electronic cash, the availability of liquid exchange markets generally guarantees some level of interoperability.

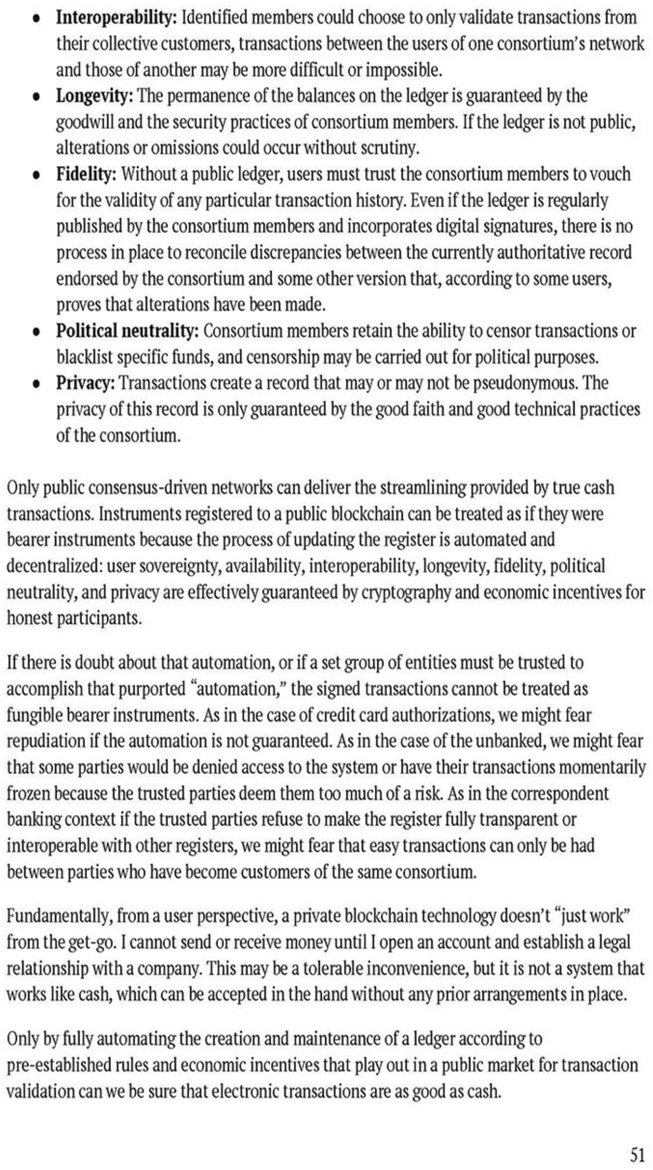


- **Longevity:** By decentralizing the storage of the ledger redundantly across all participants, and employing digital signatures to link all transactions into a unified data structure, the network ensures that even very old transactions never go missing from the ledger. Balances a user has left untouched for years or even decades are still available for spending.
- **Fidelity:** Transactions are recorded on the ledger in bundles called blocks. Transactions must obey logical rules to be incorporated into blocks (*e.g.*, spending the same bitcoins twice is not allowed). Transactions cannot be altered after the fact; any such attempted alteration would invalidate digital signatures within the block containing the transaction and in all subsequent blocks. These mismatched signatures highlight the fraud and (unless the full network of participants decide to change the network's rules against fraud) the attempt at alteration would be ignored. New transactions might be "erased" in favor of other transactions when one "block" replaces another within the most recent history of the ledger, but blocks further back in the ledger cannot be replaced without simultaneously replacing all blocks since that block, a process that would demand prohibitively costly computing resources.
- **Political neutrality:** By creating a public and global market for transaction validation and infrastructure upkeep, the network ensures that it would never be vulnerable to attempts by one government or institution to censor or stop particular transactions, or freeze particular balances. Additionally, the supply of the tokens is set by the software, and so would not be subject to the monetary policies of a state or the choices of a single corporation or institution.[102]
- **Privacy:** Bitcoin transactions *do* leave a record, but it is a pseudonymous record that generally does not make a user's full transaction history public information. The development of privacy-protecting technologies like zero-knowledge proofs or shuffling protocols may make identification of pseudonyms more difficult while also granting individuals the ability to selectively disclose information related to their transactions.

Private consensus mechanisms would make it difficult to guarantee these features:

- **User sovereignty:** The user must rely on the consortium members as intermediaries to ensure that the transaction will proceed.
- **Availability:** The identified members of the consortium could be compromised and the system could cease validating transactions or could be made to block the transactions of certain users. If the members collude they could block the transactions of certain users.

[102] Centralization of validators on an open network because of economic advantages from cooperation or geographic co-location is a real concern in these systems, however, thus far we've see little evidence of harms from this vulnerability. *See* Kyle Torpey, "Problems Associated With Bitcoin Mining Centralization May Be Overstated" *Bitcoin Magazine* (Sep. 2016) https://bitcoinmagazine.com/articles/problems-associated-with-bitcoin-mining-centralization-may-be-overstated-1474917259.



- **Interoperability:** Identified members could choose to only validate transactions from their collective customers, transactions between the users of one consortium's network and those of another may be more difficult or impossible.
- **Longevity:** The permanence of the balances on the ledger is guaranteed by the goodwill and the security practices of consortium members. If the ledger is not public, alterations or omissions could occur without scrutiny.
- **Fidelity:** Without a public ledger, users must trust the consortium members to vouch for the validity of any particular transaction history. Even if the ledger is regularly published by the consortium members and incorporates digital signatures, there is no process in place to reconcile discrepancies between the currently authoritative record endorsed by the consortium and some other version that, according to some users, proves that alterations have been made.
- **Political neutrality:** Consortium members retain the ability to censor transactions or blacklist specific funds, and censorship may be carried out for political purposes.
- **Privacy:** Transactions create a record that may or may not be pseudonymous. The privacy of this record is only guaranteed by the good faith and good technical practices of the consortium.

Only public consensus-driven networks can deliver the streamlining provided by true cash transactions. Instruments registered to a public blockchain can be treated as if they were bearer instruments because the process of updating the register is automated and decentralized: user sovereignty, availability, interoperability, longevity, fidelity, political neutrality, and privacy are effectively guaranteed by cryptography and economic incentives for honest participants.

If there is doubt about that automation, or if a set group of entities must be trusted to accomplish that purported "automation," the signed transactions cannot be treated as fungible bearer instruments. As in the case of credit card authorizations, we might fear repudiation if the automation is not guaranteed. As in the case of the unbanked, we might fear that some parties would be denied access to the system or have their transactions momentarily frozen because the trusted parties deem them too much of a risk. As in the correspondent banking context if the trusted parties refuse to make the register fully transparent or interoperable with other registers, we might fear that easy transactions can only be had between parties who have become customers of the same consortium.

Fundamentally, from a user perspective, a private blockchain technology doesn't "just work" from the get-go. I cannot send or receive money until I open an account and establish a legal relationship with a company. This may be a tolerable inconvenience, but it is not a system that works like cash, which can be accepted in the hand without any prior arrangements in place.

Only by fully automating the creation and maintenance of a ledger according to pre-established rules and economic incentives that play out in a public market for transaction validation can we be sure that electronic transactions are as good as cash.

B. Identity

The Internet lacks a native identity layer. This shortcoming is the reason why Internet users must rely on a tapestry of weak passwords, secret questions, and knowledge of mother's maiden names to verify their identity to various web service providers. The need for a better solution is widely recognized,[103] and public blockchains may provide the answer.

i. What is Identity? Why is it Difficult Online?

In the physical world, identity is *federated.*[104] In other words, we don't have just one monolithic identity; we have a host of attributes. Nor do we have just one institution that vouches or attests that we have these attributes, we have several. A person's identity includes an endless variety of attributes: physical appearance, parentage and family history, citizenship, educational and employment history, skills, personality, etc. We seek and often carry evidence that others have attested to our attributes: driver's licenses, passports, birth certificates, membership cards, diplomas, letters of recommendation, professional certifications, awards, resumes, etc. In the physical world our identity is *user sovereign*: the bulk of these credentials are things over which we have immediate physical control; we keep them in our homes or our wallets; we might even wear them on our faces. We are in control of these attestations and can choose to show or decline to show them to others at will.

Online we should expect no different. As early as 1996, the need for robust digital identity systems was glaringly apparent. As the Clinton Administration noted in its Framework for Global Electronic Commerce:

> Of particular importance is the development of trusted certification services that support the digital signatures that will permit users to know whom they are communicating with on the Internet. Both signatures and confidentiality rely on the use of cryptographic keys. To promote the growth of a trusted electronic commerce environment, the Administration is encouraging the development of a voluntary, market-driven key management infrastructure that will support authentication, integrity, and confidentiality.[105]

But creating a robust, federated, and user-sovereign identity system that works online has proven difficult. As President Obama noted in a letter introducing the National Strategy for Trusted Identities in Cyberspace ("NSTIC") program:

> The rapid and vastly positive changes that have followed the rise of online transactions – like making purchases or downloading bank statements – have also led to new

[103] *See, e.g.*, Barak Obama, *Cover letter to the National Strategy for Trusted Identities in Cybersapce* (April 2011) *available at* https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[104] *See* Eve Maler and Drummond Reed, "The Venn of Identity: Options and Issues in Federated Identity Management" *IEEE Security & Privacy* (2008) *available at* https://css.csail.mit.edu/6.858/2012/readings/identity.pdf.

[105] *See* Clinton *supra* note 8.

> challenges. Few have been as costly or nerve wracking for businesses and families as online fraud and identity theft. These crimes cost companies and individuals billions of dollars each year; and they often leave in their wake a mess of ruined credit and damaged finances that can take years to repair. But there are other costs for our economy that are more difficult to measure. The potential for fraud and the weakness of privacy protections often leave individuals, businesses, and government reluctant to conduct major transactions online. For example, providing patients with access to their medical records from their home computers requires that hospitals be able to confidently identify that patient online.
>
> The simple fact is, we cannot know what companies have not been launched, what products or services have not been developed, or what innovations are held back by the inadequacy of tools, like insecure passwords, long overwhelmed by the fantastic and unpredictable growth of the Internet.[106]

One of the key challenges has been developing an interoperable system for online identity. As the NSTIC framework specifies:

> The third guiding principle of the Identity Ecosystem is to ensure policy and technology interoperability among identity solutions, which will enable individuals to choose between and manage multiple different interoperable credentials. Interoperability will also support identity portability and will enable service providers within the Identity Ecosystem to accept a variety of credential and identification media types.[107]

Interoperability is a technical challenge that demands a public, purpose-neutral platform through which users and institutions can present credentials and offer attestations depending on their particular needs. Researchers at Microsoft have stressed that:

> [D]ifferent identity systems must exist in a metasystem. It implies we need a simple encapsulating protocol (a way of agreeing on and transporting things) ... The universal identity metasystem must not be another monolith. It must be polycentric (federation implies this) and also polymorphic (existing in different forms). This will allow the identity ecology to emerge, evolve, and self-organize. Systems like RSS and HTML are powerful because they carry any content. We need to see that identity itself will have several—perhaps many—contexts, and yet can be expressed in a metasystem.[108]

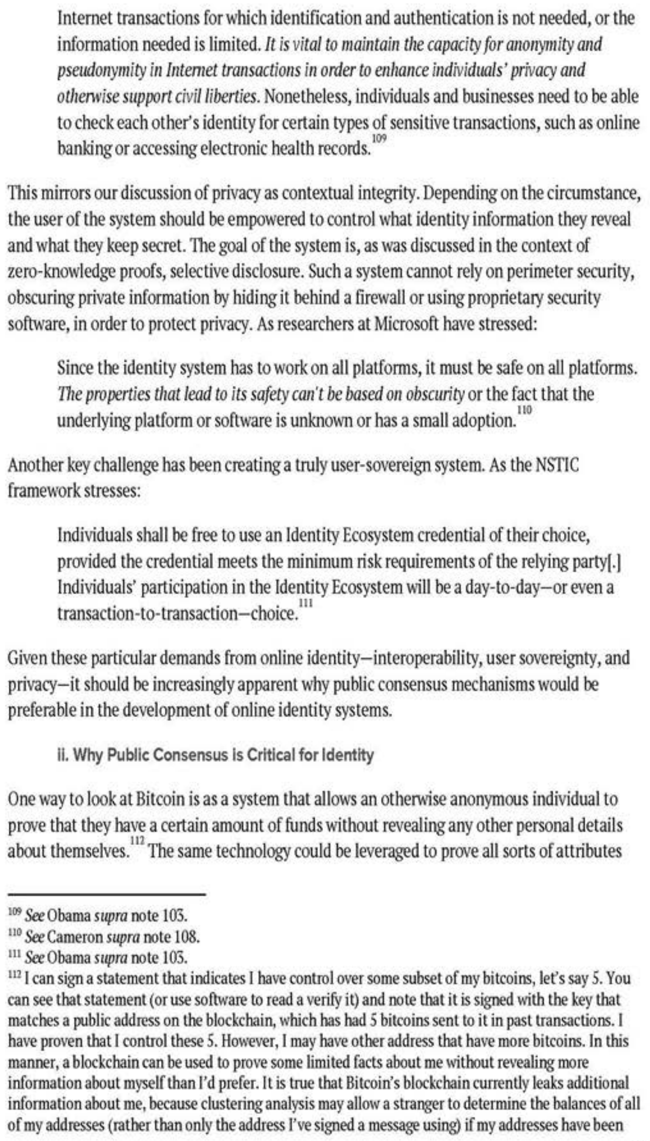
Another key challenge lies in creating a system that is privacy-protecting. As the NSTIC framework specifies:

> Just as there is a need for methods to reliably authenticate individuals, there are many

[106] *See* Obama *supra* note 103.

[107] *Id.*

[108] Kim Cameron, *The Laws of Identity* (May 2005) https://msdn.microsoft.com/en-us/library/ms996456.aspx.



> Internet transactions for which identification and authentication is not needed, or the information needed is limited. *It is vital to maintain the capacity for anonymity and pseudonymity in Internet transactions in order to enhance individuals' privacy and otherwise support civil liberties*. Nonetheless, individuals and businesses need to be able to check each other's identity for certain types of sensitive transactions, such as online banking or accessing electronic health records.[109]

This mirrors our discussion of privacy as contextual integrity. Depending on the circumstance, the user of the system should be empowered to control what identity information they reveal and what they keep secret. The goal of the system is, as was discussed in the context of zero-knowledge proofs, selective disclosure. Such a system cannot rely on perimeter security, obscuring private information by hiding it behind a firewall or using proprietary security software, in order to protect privacy. As researchers at Microsoft have stressed:

> Since the identity system has to work on all platforms, it must be safe on all platforms. *The properties that lead to its safety can't be based on obscurity* or the fact that the underlying platform or software is unknown or has a small adoption.[110]

Another key challenge has been creating a truly user-sovereign system. As the NSTIC framework stresses:

> Individuals shall be free to use an Identity Ecosystem credential of their choice, provided the credential meets the minimum risk requirements of the relying party[.] Individuals' participation in the Identity Ecosystem will be a day-to-day—or even a transaction-to-transaction—choice.[111]

Given these particular demands from online identity—interoperability, user sovereignty, and privacy—it should be increasingly apparent why public consensus mechanisms would be preferable in the development of online identity systems.

ii. Why Public Consensus is Critical for Identity

One way to look at Bitcoin is as a system that allows an otherwise anonymous individual to prove that they have a certain amount of funds without revealing any other personal details about themselves.[112] The same technology could be leveraged to prove all sorts of attributes

[109] *See* Obama *supra* note 103.

[110] *See* Cameron *supra* note 108.

[111] *See* Obama *supra* note 103.

[112] I can sign a statement that indicates I have control over some subset of my bitcoins, let's say 5. You can see that statement (or use software to read a verify it) and note that it is signed with the key that matches a public address on the blockchain, which has had 5 bitcoins sent to it in past transactions. I have proven that I control these 5. However, I may have other address that have more bitcoins. In this manner, a blockchain can be used to prove some limited facts about me without revealing more information about myself than I'd prefer. It is true that Bitcoin's blockchain currently leaks additional information about me, because clustering analysis may allow a stranger to determine the balances of all of my addresses (rather than only the address I've signed a message using) if my addresses have been

about an individual, effectively creating a user-sovereign, federated identity system.

Already some companies are experimenting with such a system. Today, for example, I can use a service called Onename, created by a company called Blockstack, to leverage the Bitcoin blockchain in helping me establish an online identity.[113] It works like this: I log into my Facebook account, my Twitter account, and my LinkedIn account and post a special message proving I control those accounts. A copy of that message is then signed with a digital signature that matches my established Bitcoin address.[114] Proof of those signatures can be encapsulated in the Bitcoin blockchain and the Onename website will make it easy for me to sign, write, and read those messages to and from the blockchain. Now, if I want to prove to someone who I am online, I can show them my signed messages on the blockchain and sign a personal message to them using the same key.

Effectively, the system allows the user to self-attest to an identity. The user shows that they have control over three different social networking profiles by creating signed attestations on each profile. A single Facebook account may be easy to fraudulently generate, but three different social media accounts, particularly if they have active use indicative of the person they purport to represent, would be harder to forge. With attestations from each account now available on the blockchain, we can be reasonably assured that any message signed with the private key matching that blockchain address is truly a message from the person who has those social media accounts.

We could imagine similar attestations from any number of federated attestors also residing as signed messages encapsulated and stored on the Bitcoin blockchain or any other public consensus blockchain. Now if want to prove I have a certain credit score, or a certain diploma, I can ask the credit rating agency or the university to sign an attestation and "transfer" it (as one would transfer bitcoins) to a public blockchain address I control. Now I can present that attestation, signing it again with my private key, to anyone curious about my creditworthiness or educational history. Because blockchains provide a sort of decentralized time-stamping, the attestation could be made to expire automatically, and subsequent on-chain messages signed by the attestor could revoke previous attestations if, say, my credit score changes or if my diploma is revoked.

These attestations could also be required of users who want to log into a given website, say an online banking account. Rather than mandating that a user create a password and use that password to log in, a bank could sign a login credential and assign it to that user's blockchain address. Now, to log in, she signs a login message with the private key that matches her blockchain address. The bank's website looks for that signed message, validates the signature,

used together in past transactions. This privacy weakness is, however, surmountable and, as discussed in the section on privacy (*see infra* at 35), several efforts are underway to make public blockchain networks more private, and capable of true granular information sharing and verification.

[113] *See* Ali *supra* note 5. *See also* https://onename.com/.

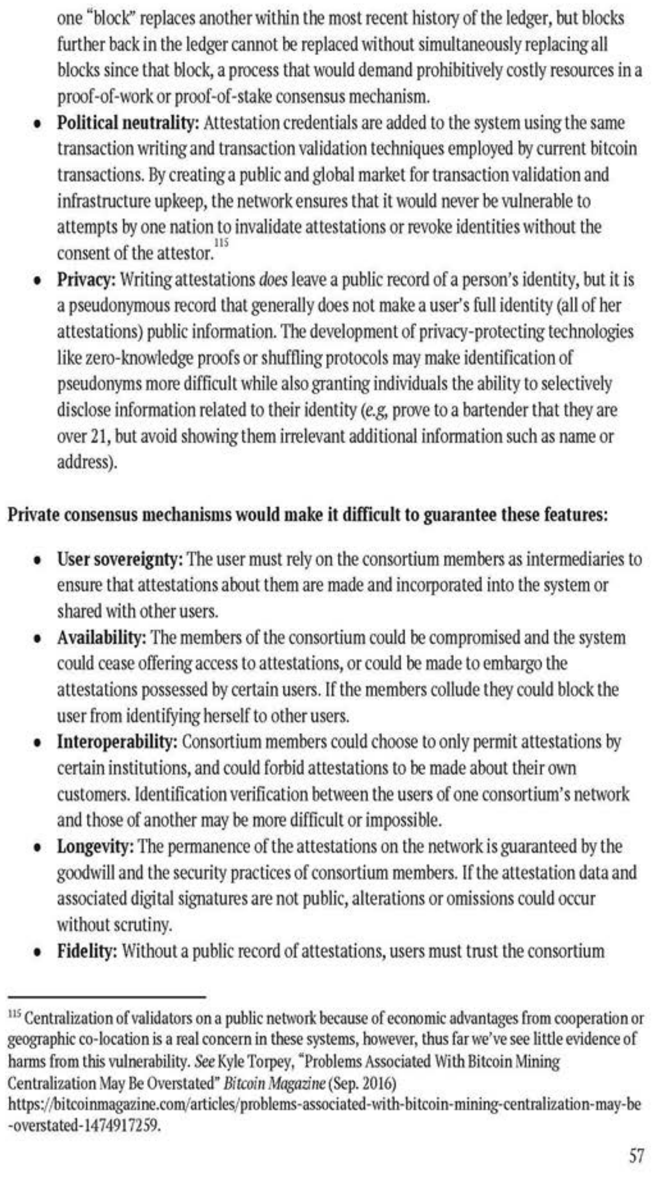
[114] *See, e.g.*, my personal Onename profile: https://onename.com/valkenburgh and an associated message I placed on my twitter profile: https://twitter.com/valkenburgh/status/595664205270880258.

and allows her to login. Reverse engineering a Bitcoin private key is effectively impossible, and that's a major step up from most user-set passwords that can be cracked in hours or even minutes by an enterprising hacker.

If the user loses her phone or laptop, her private keys could, of course, be compromised, and if she failed to keep backups she will be unable to sign messages proving her identity attestations. To solve this problem, public blockchain networks can leverage what are called multi-signature transactions. In essence, before accepting any attestation credentials at a given blockchain address, I empower three friends, co-workers, or institutions, with the ability to re-assign my credentials to another address should I ever lose my keys. Now if I lose my cell phone, I can call up my friends, ask them to revoke my credentials, and then meet with them to provision those credentials to a new address I've generated with the keys stored on my new device.

As with our discussion of electronic cash, it's now helpful to describe the key attributes offered by **public consensus mechanisms** and explain how they relate to an online identity system:

- **User sovereignty:** The bearer of a private key that corresponds to a pseudonym in control of certain identity attestations is the only party able to offer an attestation as proof of her identity, and no third party aside from the attestor who issued that attestation need be relied upon to ensure that the identification can proceed.
- **Availability:** No particular node on the network can block a user perpetually from offering attestations for identification purposes, nor would the technical failure of any particular node stop the user from offering attestations because the process of writing and reading from the digital ledger is decentralized across a network of peers.
- **Interoperability:** The user does not have to have a common relationship with any particular member of the network and the person to whom they are identifying themselves for an attestation to be shared; all software necessary to utilize and interact with the network is freely available without seeking licenses or paying fees. The user can seek attestation credentials from any individuals or institutions that choose to use the system and there is no fee or permission or establishment of any provider-customer relationship required for an attestor to join the system and start making attestations about users.
- **Longevity:** By decentralizing the storage of the attestations redundantly across all participants, and employing digital signatures to link all attestation transactions into a unified data structure, the network ensures that even very old attestations never go missing from the ledger. Attestations a user has left untouched for years or even decades are still available for proving her identity (provided they have not been set by the attestor to expire).
- **Fidelity:** Attestations are recorded on the ledger within transactions that are bundled into blocks. Transactions and their associated attestation data cannot be altered after the fact; any such attempted alteration would invalidate digital signatures within the block and in all subsequent blocks. These mismatched signatures highlight the fraud and the attempt at alteration will be ignored. New attestations might be "erased" when



one "block" replaces another within the most recent history of the ledger, but blocks further back in the ledger cannot be replaced without simultaneously replacing all blocks since that block, a process that would demand prohibitively costly resources in a proof-of-work or proof-of-stake consensus mechanism.

- **Political neutrality:** Attestation credentials are added to the system using the same transaction writing and transaction validation techniques employed by current bitcoin transactions. By creating a public and global market for transaction validation and infrastructure upkeep, the network ensures that it would never be vulnerable to attempts by one nation to invalidate attestations or revoke identities without the consent of the attestor.[115]
- **Privacy:** Writing attestations *does* leave a public record of a person's identity, but it is a pseudonymous record that generally does not make a user's full identity (all of her attestations) public information. The development of privacy-protecting technologies like zero-knowledge proofs or shuffling protocols may make identification of pseudonyms more difficult while also granting individuals the ability to selectively disclose information related to their identity (*e.g*, prove to a bartender that they are over 21, but avoid showing them irrelevant additional information such as name or address).

Private consensus mechanisms would make it difficult to guarantee these features:

- **User sovereignty:** The user must rely on the consortium members as intermediaries to ensure that attestations about them are made and incorporated into the system or shared with other users.
- **Availability:** The members of the consortium could be compromised and the system could cease offering access to attestations, or could be made to embargo the attestations possessed by certain users. If the members collude they could block the user from identifying herself to other users.
- **Interoperability:** Consortium members could choose to only permit attestations by certain institutions, and could forbid attestations to be made about their own customers. Identification verification between the users of one consortium's network and those of another may be more difficult or impossible.
- **Longevity:** The permanence of the attestations on the network is guaranteed by the goodwill and the security practices of consortium members. If the attestation data and associated digital signatures are not public, alterations or omissions could occur without scrutiny.
- **Fidelity:** Without a public record of attestations, users must trust the consortium

[115] Centralization of validators on a public network because of economic advantages from cooperation or geographic co-location is a real concern in these systems, however, thus far we've see little evidence of harms from this vulnerability. *See* Kyle Torpey, "Problems Associated With Bitcoin Mining Centralization May Be Overstated" *Bitcoin Magazine* (Sep. 2016) https://bitcoinmagazine.com/articles/problems-associated-with-bitcoin-mining-centralization-may-be-overstated-1474917259.

members as to the validity of any particular attestation. Even if the record of attestations is regularly published by the consortium members and incorporates digital signatures, there is no process in place to reconcile discrepancies between the currently authoritative record endorsed by the consortium and some other version that, according to some users, proves that alterations have been made.

- **Political neutrality:** Consortium members retain the ability to censor identity attestations, block user from asserting their identities, or blacklist specific users/identities, and censorship may be carried out for political purposes.
- **Privacy:** Writing attestations creates a record of users' identities. The privacy of this record is only guaranteed by the good faith and good technical practices of the consortium members.

In general, identity is a many-faceted concept. A person's identity is a bundle of qualities that she exhibits, and attestations that others make about her. If a centralized authority can see as well as revoke any and all of your credentials, it could present privacy and human rights issues. No such singular authority exists in the physical world where even a person denied a driver's license can still obtain a diploma, where a person denied a bank account can still get a passport, where the common infrastructure of identity is paper, plastic cards, or independent electronic records. We should expect nothing less from the digital world, and public consensus mechanisms are essential to that development.

C. The Internet of Things

The promise of the Internet of Things is that every device you own or use—every "thing" in your home and beyond—will be "smart" and "networked."[116] From light switches to door locks, thermostats to toothbrushes, street lights to cars, everything will be collecting data about its use, will have a networked interface for remote usage, and will be able to communicate as needed with users or any other devices with which it may need to coordinate. Self-driving cars will whiz through intersections because their trajectories will be intelligently coordinated with other vehicles, refrigerators will know when you are running out of eggs or when the milk's gone bad and will order more, and every appliance in your home will be able to be switched off from hundreds of miles away if you're on vacation and worried you left something on.

Whether this utopian vision is likely or even desirable goes beyond the scope of this paper. Many homes already have smart thermostats, lights, door locks, televisions, and voice assistants like Amazon's Alexa, and even with these non-speculative, early-generation IoT devices, the need for public networks to underpin their operation is becoming apparent. Additionally, non-consumer, industrial IoT usage is on the rise. For example, smart devices can enable the automated monitoring of well-head flows across an oil field, equipment safety across a construction site, or soil moisture across a farm.[117] These uses also face the same security, availability, and longevity concerns as consumer devices but the consequences of

[116] *See* IBM *supra* note 58.

[117] *See* Saint-Andre *supra* note 56.

failure can be even more dire.[118]

i. Why Public Consensus is Critical for the Internet of Things

IoT devices in general will need to identify themselves online for control and communications purposes. This means that all of the concerns we had about human identification in the previous section are again present with respect to device identification. IoT underscores the importance of decentralized identity because rather than merely being concerned with some 10 billion people who may each have multiple digital credentials (*e.g., can drive, is over 18*, or *has credit score 729*) we must now also consider that each person may have 10 or even 100 smart devices in their home, business, or under their control, and each device may have multiple identities and credentials (*e.g. this lock can be opened by these five family members and this friend and these emergency personnel in case of an emergency*, or *this car must be capable of communicating with and then programmatically sharing the road with every other car that may be traveling today*). The sheer number of device identities and credentials inherent in projections of widespread IoT deployment necessitates that no one or handful of centralized authorities be in full control of that identification system. Reliance on one or a handful of identity validators would invite fragility into a massive and critical technological system; it would entrust reams of private data to a small group of actors who could engage in abusive or anti-competitive business practices or else become the target of devastating hacks.

Similarly, devices may need to shop and make payments. This is already the case for voice assistants like Amazon's Alexa, which can be used to shop for and buy consumer goods by voice interaction alone. This brings us back to several of the issues we encountered in the section on electronic cash. Payments, including device payments, should be under the control of the person whose value is at stake, the user. A device manufacturer need not retain the ability to block payments or accumulate private payments-related data merely because they sold you a piece of IoT hardware. A ride-sharing application developer should not necessarily retain the ability to limit your selection of possible drivers or prices merely by limiting the markets for drivers that your smartphone is capable of accessing. Consumer choice, privacy, and payment security can be bolstered if our connected devices can shop for us via decentralized markets powered by decentralized payment systems.

In previous sections we've looked at seven attributes of public consensus mechanisms and investigated how a particular use case may require these attributes. Rather than rehash all seven attributes here again, this section will focus on four that have particular importance in the IoT context: longevity, user sovereignty, privacy, and interoperability.

Longevity. A recurring annoyance for IoT pioneers (brave souls who have, say, already replaced all of their lightbulbs with smart bulbs) is unexpected or rapid "sunsetting" of a product by its manufacturer. This refers to a decision by the manufacturer to end technical or infrastructural support for the product. Within the realm of non-smart products, an end to

[118] *See, e.g.*, Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon" *Wired* (Nov. 2014) https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

manufacturer support can already be troublesome because customer service and repair may now become more difficult, but in the realm of smart products an end to support can be significantly worse.

A smart product will often only function properly when it is capable of connecting to and communicating with a server on the Internet that may, among other things, (A) help it identify itself and connect to other consumer products or Internet services,[119] (B) provide a web- or app-based user interface for the user to control the product's features,[120] and/or (C) store and process data essential to the device's operation.[121] That server will generally be operated and maintained by the device manufacturer and, should the manufacturer decide to take that server offline, the device may cease proper operation. This has been the case even with seemingly simple smart home products like light bulbs.

Take for example issues surrounding bulbs manufactured by Connected by TCP.[122] These bulbs were marketed as being compatible with other smart-home systems, in particular the Amazon Echo voice assistant (so that you could say, *e.g.*, "Alexa, turn on my kitchen lights")[123] and a mobile app called Wink that offers a dashboard for user control over a variety of smart devices (so that you would not need to navigate to various different apps on your phone to control devices made by different manufacturers).[124] The bulbs were also marketed as being capable of remote control over the Internet (so that you could turn them on and off even when out of the range of your home Wi-Fi network). Compatibility and remote control for the Connected by TCP bulbs was provided via a web server that was owned, maintained, and under the full control of Connected by TCP. The server would relay signals for switching the bulbs on and off from a user's Amazon Echo or Wink app to the user's Connected by TCP light bulb hub, and then, in turn, to the bulbs themselves.

In June of 2016, after years of selling these bulbs, Connected by TCP abruptly decided to take their server offline.[125] With the critical relay path to the bulbs now missing, all remote functionality and device interoperability disappeared. As a writer for Consumerist wrote:

> The bulbs still work as actual lightbulbs, if you want to use your lamp's on-off switch the old-fashioned way, and you can control them while inside the house on your home

[119] *See* Tobias Heer, *et al.*, "Security Challenges in the IP-based Internet of Things" *Wireless Pers Commun* (2011) *available at* http://link.springer.com/article/10.1007/s11277-011-0385-5.

[120] *Id.*

[121] *Id.*

[122] *See* Kate Cox, "TCP Disconnects "Smart" Lightbulb Servers, Leaves Buyers In The Dark" *Consumerist* (Aug. 2016) https://consumerist.com/2016/08/19/tcp-disconnects-smart-lightbulb-servers-leaves-buyers-in-the-dark/.

[123] *See* Michael Garcia, "Using Alexa Skills Kit and AWS IoT to Voice Control Connected Devices" *Amazon Developer* (May 2016) https://developer.amazon.com/blogs/post/Tx3828JHC7O9GZ9/Using-Alexa-Skills-Kit-and-AWS-IoT-to-Voice-Control-Connected-Devices.

[124] "Wink Hub" *Wink.com* http://www.wink.com/products/wink-hub/ *last accessed* Dec. 2016.

[125] *See* Cox *supra* note 122.

> WiFi network. But any remote functionality—a big part of the steep price tag that makes TCP bulbs more expensive than a plain old LED bulb—is long gone.
>
> The fact that the bulbs are still on store shelves, with packaging promising features that no longer exist, is irksome. But it's also not an uncommon tale in these early years of the Internet of Things. Businesses try, and then discontinue, new products all the time.[126]

The Federal Trade Commission has taken a careful look at this burgeoning problem, launching an investigation into Google's choice to end support for products manufactured by Nest, a smart-home firm it acquired.[127] The FTC ultimately closed that investigation but warned manufacturers of their concern over two key policy issues:

> First, there are serious issues at play when consumers purchase products that unexpectedly stop functioning due to a unilateral decision by the company that sold it. Consumers generally expect that the things they buy will work and keep working, and that includes any technical or other support necessary for essential functioning.
>
> Second, when a company stops providing technical support, including security updates, for an IoT device, consumers may be left with an out-of-date product that is vulnerable to critical security or privacy bugs. This could create vulnerabilities for other systems connected to these IoT devices, and put consumers' sensitive data at risk. And if hackers can hack a smart car, pacemaker, or insulin pump, the risks are even more serious.[128]

Public consensus mechanisms can provide significantly enhanced longevity by replacing a privately owned and maintained server with a decentralized computing network. Device identity and data storage can be be offloaded to a decentralized ledger and decentralized file system and the device can even be pre-loaded by the manufacturer with a modest amount of funds to pay the global network of parties contributing resources to that decentralized network for the device identity registration, data storage, and connectivity that it needs for a reasonable lifetime. Now, even if the manufacturer goes out of business, if it decides to change its product offerings, or is acquired by a company unwilling to continue device support, the device itself will continue to have the same network infrastructure necessary to maintain proper functioning.

A private consensus mechanism may not provide this guarantee of longevity. The consortium members, just like the company with a centralized server, may choose to deprecate support for older products, or they may shut down the network entirely. Only a public network where participants are free to come and go and are incentivized to participate by device payments

[126] *Id.*

[127] Jessica Rich, "What happens when the sun sets on a smart product?" *FTC Business Blog* (Jul 2016) https://www.ftc.gov/news-events/blogs/business-blog/2016/07/what-happens-when-sun-sets-smart-product

[128] *Id.*

will assuredly continue to function for as long as devices continue to pay. Additionally, if the device's on board wallet is pre-loaded with electronic cash powered by a public blockchain network, then reloading the device with new funds is a simple process that anyone in possession of the device (perhaps even after multiple resales) could accomplish.[129]

User sovereignty and privacy. Nobody wants a baby monitor, security camera, or even a remote-activated light bulb that several dozen complete strangers may be able to access and control. In the world of "dumb" devices this was easy for a device designer to avoid: unless you have physical access to the switches on the device, you have no control over its operation. So a baby monitor that is closed-circuit or that only broadcasts analog signals will generally be in the sole and sovereign control of people in the house. Assume there are locks on the doors and we have good user-sovereignty and privacy.

Smart, internet-connected devices, however, when they rely on web servers for their functionality, will often fail to have these qualities. Recall Nick Szabo's characterization of the web's client-server architecture:

> When we currently use a smartphone or a laptop on a cell network or the Internet, the other end of these interactions typically run on other solo computers, such as web servers. Practically all of these machines have architectures that were designed to be controlled by a single person or a hierarchy of people who know and trust each other. From the point of view of a remote web or app user, these architectures are based on full trust in an unknown "root" administrator, who can control everything that happens on the server: they can read, alter, delete, or block any data on that computer at will.[130]

This applies to any device in the home that connects to the Internet as well as it does to a smartphone or laptop. Let's imagine a baby monitor that can be switched on and off remotely, and that broadcasts audio and video to the user's smartphone. Generally, these devices are manufactured to use a client-server architecture.[131] The logic of the application (rules for how and when the device should turn on, rules for who has access to the device, rules for how data from the device should be routed) exists on a server controlled and maintained by the device manufacturer and physically remote from the device (probably in a large data center somewhere).[132]

The user connects the baby monitor to the Internet using the home's wired or Wi-Fi connections and the device, in turn, connects to the manufacturer's web server; the baby monitor is now one client of the server. The user then sets up her smartphone with an app provided by the manufacturer for controlling the baby monitor and viewing the feed. The user's device is *another* client of the server. When the user decides to switch on the monitor from her cell phone, a message is sent to the server, checked for authenticity, and then relayed

[129] *See infra* at 45.
[130] *See* Szabo *supra* note 2.
[131] *See* Heer *supra* note 119.
[132] *Id.*

to the device itself. The baby monitor turns on. Unlike a light switch that completes a circuit entirely within the home, this "circuit" exists across potentially hundreds of miles of Wi-Fi, cellular signal, satellite, fiber-optic cable, and server warehouse. Similarly, when the baby monitor relays a video feed of baby, that data travels back across the Internet, to the server, and then back to the user's device (this may be the case even when the user is in her own home and near the monitor).

This system architecture presents a major issue from a user-sovereignty standpoint. Unless the application server is very carefully designed, someone with physical access to that server may be able to control the baby monitor as easily as the user can from her cell phone. Indeed, if the application server is poorly designed (*e.g.* firewalls are not well employed, user passwords are not strong and properly stored, encryption is not used to mask data coming and going from the server, and/or streaming protocols are employed without password-protection) then anyone in the world with an Internet connection may be able to control the baby monitor.

This is not as rare of problem as it may sound. Indeed, there is a search engine, Shodan,[133] that can be used to comb the Internet for connected devices that promiscuously broadcast unprotected video feeds, as reported by Ars Technica:

> Shodan, a search engine for the Internet of Things (IoT), ... includes images of marijuana plantations, back rooms of banks, children, kitchens, living rooms, garages, front gardens, back gardens, ski slopes, swimming pools, colleges and schools, laboratories, and cash register cameras in retail stores, according to Dan Tentler, a security researcher who has spent several years investigating webcam security. "It's all over the place," he told Ars Technica UK. "Practically everything you can think of."[134]

Off-loading as much device registration and application logic as possible to decentralized systems should provide enhanced user-sovereignty. This may be relatively straightforward when it comes to authentication. As discussed in the section on identity, the user can provision herself (*e.g.* her smartphone) and the smart device with identity credentials and access rules that would reside on the blockchain. The device can always query the blockchain for a current list of authorized users (*e.g.*, pseudonyms that must sign with matching private keys to gain access) and users can rely on multi-sig setups to revoke credentials if their smartphone is lost or stolen.

Data from the device, say video feeds from a security camera, can be encrypted and stored locally or in a decentralized file system[135] where members of the network provide surplus storage in return for payments from devices. So long as the keys to the encrypted data remain

[133] Shodan, https://www.shodan.io/ *last accessed* Dec. 2016.

[134] J.M. Porup, "*'Internet of Things' security is hilariously broken and getting worse*" ArsTechnica (Jan. 2016) http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/.

[135] *See, e.g.*, IPFS, https://ipfs.io/ *last accessed* Dec. 2016.

with the user, none of these otherwise anonymous storage providers will be able to access or view the encrypted files.

Computing tasks that the device may need to perform in order to function, say analyzing video data to find human faces or identify intruders, can be designed to run locally on the device only, rather than on a server. Alternatively, those computing tasks could also be offloaded to a decentralized computing network[136] where participants offering computing services are rewarded by payments from the device for data processing. In this case, of course, no private data should be shared with the decentralized network unless it is encrypted. This may appear to limit the value of a decentralized computing network: how can the network process the data if it cannot view it unencrypted? The science of distributing computing work amongst several participants without fully revealing encrypted data data is a vibrant and growing subfield within cryptography, generally referred to as *secure multiparty computation*.[137]

One technique in this field is the development of robust *homomorphic encryption*,[138] which means that a computation performed on an encrypted file will yield the same result as a computation performed on a plain text (not encrypted) file. So in our video analysis example, the decentralized network can still process the video data and give a result: *in this 12 hours of video there was one human intruder who entered the house*, but the various maintainers of the several computers that may have been involved in that decentralized data processing cannot ever see the unencrypted video file and therefore cannot ever see any details about the device-user's home (aside from knowing that there was one human intruder within a given time, as per our example).

Zero-knowledge proofs provide another cryptographic tool used to achieve this level of privacy.[139] As described previously, a ledger of transactions can be effectively encrypted or hidden but a zero-knowledge proof can still process the data in that ledger and reveal whether any transactions attempted to double spend funds. In this sense a public ledger can still be privacy protecting while still guaranteeing that all transactions were valid and not counterfeit. This can work in the IoT context as well. Rather than "all transactions were valid," the limited proof is "all smart lock door openings were from authenticated users," and only this data becomes public not the specific times that the door was opened or the identities of the authorized lock openers.

Another tool to build these system architectures is the division of computational work into several small pieces and the assignment of that work across several unaffiliated participants none of whom can see the entire file being processed and, therefore, see the private data undergoing computation. The Enigma Project out of MIT is an effort to build just such a secure

[136] *See, e.g.*, Ethereum, Buterin *supra* note 6.

[137] *See* Yehuda Lindell and Benny Pinkas, "Secure Multiparty Computation for Privacy-Preserving Data Mining" *Journal of Privacy and Confidentiality* (2009) *available at* http://repository.cmu.edu/cgi/viewcontent.cgi?article=1004&context=jpc

[138] *See id.* at 79.

[139] *See id.* at 76.

multi-party computation system that relies on a blockchain to divide work into pieces, keep track of the pieces, find participants, and assign work among them.[140] This avoids reliance on a single trusted intermediary to achieve the division, a potential vulnerability if that intermediary can reassemble the pieces and see the private data being processed.

In general, the computation, data storage, and network access rules currently found within a server-client architecture for smart home devices could be decentralized by using public consensus mechanism driven networks. In theory, a private consortium driven network could achieve similar results. However, this reintroduces trust in the identified members of the consortium, weakening the goal of pure user-sovereignty.

Interoperability. Smart devices need to interact with other smart devices. The door sensor needs to communicate with the smart bulbs in order to make the hall lights come on if you come home after dark. Self-driving cars need to communicate with other self-driving cars if they are going to have smart collision avoidance and traffic pattern automation. An Amazon Alexa or similar voice controlled assistant needs to communicate with digital music retailers in order to let you shop for new music by voice.

Herein lies, perhaps, the most common sense argument for using public consensus mechanism networks to power devices in the Internet of Things. If the infrastructure powering a smart device is owned and controlled by one particular manufacturer, integrating that device with other devices may be difficult. Worse, that integration may be made deliberately difficult to gently cajole the customer into buying all of their devices from one manufacturer. This is the issue of so-called *walled gardens* in computing systems: everything is beautifully manicured but you can't leave.[141] If customers cannot choose competing products without suffering the substantial switching costs inherent in replacing *all* of their IoT devices, free and open competition suffers, and prices rise.[142]

This is particularly the case with devices that deal with online shopping. Take Amazon Echo for example. This voice assistant allows the user to order products merely by asking for them. Simply say, "*Alexa, buy me some cat litter!*" and the device will look at your past shopping habits, propose a brand, amount, and price, and allow you to agree or ask for another option. There is a fascinating and undeniably convenient feeling associated with truly hands free shopping.

But, of course, having an Alexa in your home will mean you are locked in with one retailer, Amazon, for any and all hands-free shopping that you do. When Alexa queries your shopping history and the varieties of cat litter on offer, she only shops Amazon's suppliers and partner merchants. Similarly, if you ask Alexa to play music, she will only be able to play songs you

[140] Guy Zyskind, Oz Nathan, Alex "Sandy" Pentland, *Enigma: Decentralized Computation Platform with Guaranteed Privacy*, (Dec. 2015) http://www.enigma.co/enigma_full.pdf

[141] *See* Richard Firth, "Beware the walled gardens" *itWeb Open Source* (Mar. 2013) http://www.itweb.co.za/index.php?option=com_content&view=article&id=62788.

[142] *See* Carl Shapiro & Hal r. Varian, *Information Rules: A Strategic Guide To the Network Economy* 109-10 (1998) (discussing strategies to deter customer mobility by imposing switching costs).

bought or uploaded to your Amazon account; she can't play from the collection you've amassed on, for example, iTunes. Ideally, a device would be able to access any of the digital property the user has previously purchased, and it should comparison shop across all willing sellers for things the user has yet to buy, selecting the best price for the item she wants. This open competition can only be achieved if the markets for buying and selling are truly decentralized.

Several firms are building the tools to accomplish just such decentralized commerce; one that warrants highlighting in this testimony is OpenBazaar.[143] OpenBazaar is, in essence, a decentralized eBay where buyers and sellers can find each other and engage in a safe exchange. Buyers and sellers are protected from fraud on OpenBazaar by leveraging multi-sig bitcoin transactions to place funds in a sort of trust-minimized escrow while goods are in transit or being evaluated for quality. In the event of a dispute a neutral third party arbitrator is invoked who can redirect the funds to either the seller or the buyer based on their decision regarding who was in the wrong in the disputed transaction. Additionally, OpenBazaar uses BlockStack's decentralized identity tools to create and authenticate the identities of buyers and sellers, and may soon use a decentralized files system, IPFS,[144] to host images and descriptions of items listed for sale. The result is an online shopping experience just like eBay, but it can exist on decentralized network where there is no company like eBay that has any control over the sales that occur on their platform.

There is not a good case for using regulation to force device manufactures to participate in public decentralized markets; walled gardens can have their appeal and regulations can have unintended consequences. However, it's important for policymakers to understand the potential value decentralized networks provide in fostering open digital exchange and commerce that could be foundational to better, future IoT systems.

Altogether, the case for having public consensus mechanisms power IoT blockchain networks is clear and linked to our prior discussion of identity and electronic cash. First, public blockchain networks allow for a truly decentralized data-structure for device identity (I am a bulb in this home) and user access authorization (user with address 0xE1A... is the only person who can turn me on and off). The redundant and decentralized nature of data on these networks can ensure that these systems have true longevity, and a manufacturer's decision to end support for a product will not destroy the user's ability to securely access the product's features. Second, public blockchain networks can ensure that devices are interoperable and compatible because critical infrastructure for device communication, data storage, and computation can be commoditized and shared over a peer-to-peer network rather than be owned (as a server warehouse is owned) by a device manufacturer that may be reticent to opening its costly platform to competitors. Third, device payments for supporting and maintaining that networked infrastructure or allowing the device's user to easily engage in online commerce can be made efficient by utilizing the electronic cash systems that only

[143] OpenBazaar, https://openbazaar.org/ *last accessed* Dec. 2016.
[144] IPFS, https://ipfs.io/ *last accessed* Dec. 2016.

public consensus mechanisms can facilitate.

V. Conclusion

All new approaches to decentralized computing—whether private or public—should be celebrated and allowed to develop relatively unfettered by regulatory or government policy choices. Much as the Clinton Administration took a light-touch approach to the development of the Internet in the 1990s, so should policymakers approach these new systems, however designed.[145]

In order to make good policy choices and ensure that the U.S. remains competitive in a global technological market we need a more detailed and productive discussion of these new tools. We need a basic understanding of how consensus works, what it might help us build, and why public and pseudonymous networks, despite their easily apprehended risks, offer significant and otherwise unattainable benefits. This testimony has offered a non-technical explanation of key variables within consensus mechanism design, catalogued why public mechanisms may, for certain use cases, be more worthy of user trust and more capable of ensuring user privacy and security.

The benefits of this technology are real. Electronic cash promises efficient microtransactions and enhanced financial inclusion; robust digital identity may solve many of our online security woes and streamline commerce and interaction online; and blockchain-driven Internet of Things systems may spur greater security, competition, and an end to walled gardens of non-interoperability for connected devices. However, our three highlighted use cases are likely only the tip of the iceberg. Just as few would have predicted the emergence of Facebook or Uber given only an understanding of the Internet circa 1995, it is impossible to know what creative and diverse minds will build when offered a free and public platform for experimentation.

[145] *See* Clinton *supra* note 8.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR HELLER FROM PETER VAN VALKENBURGH

Q.1. In your opinion are cryptocurriencies a security or a commodity?

A.1. Typically the term cryptocurrency refers to completely decentralized digital currency networks and their related scarce tokens, like Bitcoin and Ethereum, that have no issuer and no central party that controls these networks. These are commodities and not securities. The SEC has made it clear that Bitcoin is not a security, while the CFTC treats it as a commodity.

Q.2. How does the current regulation of cryptocurrencies in the United States compare to what other countries are doing?

A.2. The Library of Congress has published a comprehensive breakdown of cryptocurrency regulation nation-by-nation, we recommend this as a resource to the Senator if he has country-specific questions.[1] Approaches by the G20 member states vary, however, application of existing Anti-money laundering controls to financial institutions dealing in cryptocurrencies, as FinCEN did in 2013, is a common approach. We do not believe that nations should "eliminate the anonymity" that cryptocurrencies may afford; to do so would harm the legitimate privacy interests and rights of citizens. Rather, we believe that states should balance the rights of their citizens to privacy against the need for law enforcement to obtain information about criminal activities. This balance has already been struck in the context of existing forms of money, like cash transactions, and mere application of these same laws to financial institutions dealing in cryptocurrency is the best path forward. FinCEN has already offered guidance explaining why existing laws apply and all major U.S. cryptocurrency exchanges of which we are aware now comply with these data collection obligations. The worse case is for these developers to be forced overseas through bad policy.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR SASSE FROM PETER VAN VALKENBURGH

Q.1. Blockchain, or decentralized computing, clearly has the potential to be disruptive to traditional banking operations, but it can also enhance our efforts to rein in money laundering.

Q.1.a. How does the investigative process for tracking down criminal money on the public Bitcoin network compare with our methods for tracking down criminal money within traditional financial institutions?

[1] *https://www.loc.gov/law/help/cryptocurrency/world-survey.php?loclr=ealrr.*

A.1.a. In several ways, transacting with Bitcoin is far more public than transacting using the legacy financial system. Banks, although obligated under law to identify customers, may nonetheless (A) keep imperfect records of transactions; they may (B) fail to maintain records from many years ago; and (C) there will be several banks with independent records in unique data formats that must be obtained, aggregated, and merged in order to get a full picture of a person's financial history. Bitcoin, by contrast, (A) has a perfect record of all transactions made globally (because if a transaction is not in the blockchain it does not exist), (B) has a record that is maintained from the start of the network in 2009 to the present with full copies kept redundantly across several tens-of-thousands of independently owned computers the world-over, and (C) has a single record that is complete rather than partial records scattered across several institutions. Finally, Bitcoin transactions are far more transparent than physical cash transactions, which leave no record whatsoever.

Q.2. Will FinCEN's regulatory approach, requiring cryptocurrency exchanges to know their customers and engage in suspicious activity reporting, lead to the stifled growth of cryptocurrencies, as their main appeal for users is their anonymity and decentralization?

A.2. No. These technologies offer several benefits beyond anonymity. Interoperability is just one of many other benefits. Using cryptocurrency hardware and software developers have instant access to payment networks that can be built into their consumer products (even a smart light bulb can have a Bitcoin wallet and verify Bitcoin payments) without any need to seek and maintain a relationship with a bank or payments provider. We have a paper, Open Matters, that goes into this issues in greater detail.

Q.3. At what point of regulation would cryptocurrencies fail to provide any real or perceived advantages over existing currencies?

A.3. The primary value of cryptocurrencies is not their lack of regulation. Their primary value stems from the fact that they are natively digital, easy for machines to interoperate with, worthy of trust even if there is no trusted party within the system, and available to users with nothing more than free software and an internet connection. Unless regulation quite literally banned persons from using these tools (and perhaps even then) they will always have certain advantages over existing currencies.

Q.4. Mr. Valkenburgh, is there a danger if other countries decide not to follow America's lead in classifying these exchanges as money services, considering our lack of control over this global currency?

A.4. Those who would use these tools for crime will find ways to access exchanges overseas and do their business on unregulated and unsurveiled platforms. If approaches differ overseas, there will be gaps in law enforcement's ability to track cryptocurrency payments just as the same would be true with respect to traditional financial networks.

Q.5.a. Will blockchain change the way Government agencies work, including how census data and public records are stored and maintained?

A.5.a. Public blockchain networks may allow for greater integrity and transparency of records, just as the Bitcoin blockchain provides integrity and transparency of records related to Bitcoin transactions.

Q.5.b. If so, how far out are we from these practices, in your opinion?

A.5.b. We do not believe that blockchain technology is yet mature enough to warrant wide implementation in the public sector. Premature adoption could mean poor security for public data and it could also result in agencies adopting technological means that are rapidly made obsolete by newer developments. We've yet to see clear technological winners and losers in this space and much remains uncertain. This is a necessary stage in the evolution of new technologies. Just as the Government should not have immediately switched to email systems for messaging in the 1970s or immediately to the web for public communications in the 1990s, Government should carefully watch but generally not use public blockchain networks today. Limited pilot programs may prove the best approach. These systems required about 20 years maturation before they were truly ready for widespread public sector usage. Perhaps a similar time horizon is likely here, however prediction is difficult, especially about the future.

Q.6.a. What about efforts to move health records to the blockchain ecosystem, particularly as interoperability continues to be an issue in this space?

A.6.a. This would be a good use case given that the health record issue primarily revolves around the need for a universal log of access permissions over records that can be transactions (*e.g.,* one doctor granting another permission to view a chart) and interoperable between several otherwise mutually mistrustful (from a data-security standpoint) institutions and persons including hospitals, issurers, governments, and patients. However, privacy over health data and availability of data in emergencies is paramount and public blockchain networks may not yet be mature enough to warrant such critical usage.

Q.6.b. In your view, should Government play a role in facilitating this exchange of date?

A.6.b. We believe it is still premature for Government to play a role in promoting usage of public blockchain networks for critical information such as patient records.

Q.7. Where is there potential for blockchain technology outside of financial services?

A.7. Public blockchain networks have great potential to improve security and competition within the growing Internet of Things. Firstly, open blockchain networks allow for a truly decentralized data-structure for device identity (a bulb in this home's kitchen) and user access authorization (the user with address 0xE1A . . . is the only person who can turn me on and off). The redundant and decentralized nature of data on these networks can ensure that these systems have true longevity, and that a manufacturer's decision to end support for a product will not destroy the user's ability to securely access the product's features. Second, open blockchain networks can help ensure that devices are interoperable and compatible because critical infrastructure for device communication, data storage, and computation can be commoditized and shared over a peer-to-peer network rather than be owned (as a server warehouse is owned) by a device manufacturer that may be reticent to opening its costly platform to competitors. Last, device payments for supporting and maintaining that networked infrastructure or allowing the device's user to easily engage in online commerce can be made efficient by utilizing the electronic cash systems that only open consensus mechanisms can facilitate. For more, please see our paper Open Matters.

Q.8. Does the explosion of FinTech and digital payment systems compliment an emerging crypto market or detract from its usefulness?

A.8. The explosion of FinTech systems underscores the importance of cryptocurrency and public blockchain technology. As we move to a world where all economic activities will be mediate through digital payments platforms we risk an erosion of our privacy and autonomy. If massive centralized databases are used to record and mediate payments rather than blockchains, the administrators of these databases will become incredibly powerful and also incredibly vulnerable to cyber attack. For example China's economy is increasingly cashless. Cash accounted for 96 percent of payments in 2012, today that number is below 15 percent. Today mobile payment platforms like AliPay and WePay account for over $16 trillion annually—over 100 times than in the United States. Everything you buy is noted by these financial intermediaries and can be used as an input to your Social Credit score. As an Alibaba executive told a Chinese magazine in 2015, the company judges the purchases consumers make. "Someone who plays video games for 10 hours a day, for example, would be considered an idle person, and someone who frequently buys diapers would be considered as probably a parent, who on balance is more likely to have a sense of responsibility." This is a self-evident threat to the privacy of citizens but it also jeopardizes their freedom and autonomy. The centralization of these platforms and the unavailability of cash alternatives means that a citizen disfavored by his government (perhaps a bit too idle) can, with little effort, be blocked from transacting and systematically excluded from economic life.

Q.9. Some say that cryptocurrencies are more secure from privacy attacks than traditional currencies given their decentralized, anonymous nature and use of a private key, with individuals alone maintaining access to their data. Others counter that these same features actually make these currencies less secure.

Where do you fall on this spectrum and what evidence supports your viewpoint?

A.9. Cryptocurrencies are more secure from attacks than traditional currencies because transactions occur on a public blockchain (thefts are immediately evident) and individuals can control their own keys (meaning that no single organization's negligence would inherently endanger everyone's security). That said, once cryptocurrency is stolen, there is no centralized party who can reverse the transactions. Thus while these tools may be less vulnerable to attack; attacks may be harder from which to recover.

Q.10. Currently, it appears that many users view cryptocurrencies more as an investment opportunity than a viable, useable currency. Cryptocurrency is highly volatile and lacks any substantive backing. Our fiat currency, while not tethered to a material commodity, is backed by the Federal Government and is partly secured by its usability as a payment for taxes.

Can crypto, as a purely digital currency with no backing, ever be practically and reliably used as a common currency?

A.10. Even with its current volatility Bitcoin can be useful as a store of value or as a currency substitute in regions of the world where sovereign currencies have been debased or are otherwise unavailable to persons wishing to transact. Similarly, even with its current volatility these currencies may be superior for micropayments (which are non-economical if interchange fees are larger than the amount being transacted) or for machine-to-machine payments (because devices cannot have bank accounts). It's difficult to speculate about the future of digital currency volatility, just as all economic prediction under uncertainty is fraught. However, we could imagine that if a large number of persons used these currencies for payments and wealth storage rather than as speculative investments, the volatility may smooth.

Q.11.a. You've stated that Vitalik's trilemma is a challenge and not an impossibility.

Can you expand, conceptually, on how a system could be scalable, decentralized and secure?

A.11.a. Several efforts are underway to achieve these values simultaneously. We can discuss Bitcoin alone to give an example. Bitcoin is already highly secure. While individual exchanges with poor security practices have been hacked, the blockchain itself has never been hacked. Bitcoin, however, lacks some level decentralized because of the concentrated power of proof-of-work miners, but solutions are already being implemented to address this issue.

Currently the lumpy bits of Bitcoin's mining distribution are made up of powerful "mining pools." Several individual or business miners will voluntarily join a pool in order to obtain more smoothed out payments than if they mined by themselves. A single miner working alone may win a new block reward once every 2 years but several working together will win regularly and can divide the profits pro rata amongst themselves. A pool administrator is the entity who shows up on the blockchain as generating the blocks for the pool—so one administrator may seem to have 20 percent of the mining power but she is merely aggregating mining power from hundreds of participants. If a pool administrator attempts to attack the network or simply is considered too powerful then individual people tend to leave the pool, meaning that administrator's share of power in the system declines. This is a natural check on too much centralization. The root cause of this problem, however, is that the pool administrator is the one who chooses which transactions to put into a block. This is why a powerful pool could afford its administrator the ability to censor transactions. There's already a fix for this, however, and it's called BetterHash. In BetterHash pools, the individual participants of a pool get to choose which transactions they want to include when they perform the work and send it to the administrator. Thus the administrator has no ability to censor transactions and only plays a role in smoothing economic returns for participants. This decreases the centralization of Bitcoin without decreasing scalability or security.

Similarly, the Lightning Network increases scalability but does not require increased block sizes to accomplish that feat. Larger blocks would increase the infrastructure costs of mining which would inherently increase centralization (fewer parties can afford the higher fixed costs of getting started), so Lightning can enable scalability without increasing centralization. BetterHash and Lightning are merely two examples of technical solutions to Vitalik's trilemma. It is a challenge being addressed by brilliant developers, not an impossibility.

Q.11.b. How far away are we from developing such a system and is there a place for cryptocurrency without it?

A.11.b. This is difficult to predict. It was impossible to stream high definition video over the internet in the early 1990s but many had reasonable predictions that it would eventually work. Even without the scalability or decentralization improvements described above, cryptocurrencies like Bitcoin can play an important role as a store-of-value for persons without access to traditional financial tools and networks, or persons looking to hedge risks inherent in those networks.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR COTTON FROM PETER VAN VALKENBURGH

Q.1. The United States has long been the world's most appealing market for development and innovation, creating economic opportunity for millions of people. Within the cryptocurrency space however, the United States appears to be lagging behind other countries in the race to become the development and innovation leader.

Perianne Boring, president and founder of the Chamber of Digital Commerce, said in a June New York Times piece that our current crypto regulatory regime is, "unorganized and incredibly complicated," Michael Arrington, founder of Arrington XRP Capital, said recently that he will cease investing in American companies, "until the SEC clarifies token rules." He further stated he is looking to move his operations out of the United States due to the regulatory uncertainty surrounding the space.

In order to make the United States a market leader, should the SEC create a sandbox that allows for regulatory experimentation and innovation in the currency and blockchain market?

A.1. The best thing the SEC can do to make the United States a market leader is to create greater regulatory certainty around their application of securities laws to tokens. Specifically, the SEC should clarify that securities laws do not apply to functional tokens powered by decentralized networks (*e.g.,* Bitcoin, Ethereum, and others) but do apply to promises of future tokens made by promoters to investors. By and large, the recent statements of Director Hinman and the remarks of Chairman Clayton create this certainty. We do not prefer a sandbox approach because it, by necessity create bespoke regulatory standards for individual companies, eroding the uniformity of the rule of law and offering preferential treatment to select firms.

Q.2. Most Americans want to work in legitimate blockchain and cryptocurrency operations. Is our legal system set up to make American the best place to be?

A.2. Our constitutional protections for free speech and prohibitions on warrantless search make America a welcoming home for developers of cryptocurrency and public blockchain software. However, two policies could be improved to make the United States more friendly to innovators. The State-by-State licensing regime for money transmitters has costly redundancies and inappropriately tailored compliance obligations.[1] Tax policy could also be improved, even small transactions in cryptocurrency trigger capital gains tax such that basis must be calculated and taxes paid whenever minor purchases, *e.g.,* a cup of coffee, are made using cryptocurrency.[2] Finally, while the current policy of the SEC with respect to classifying tokens as cryptocurrencies as securities is wise, as described above, it could be codified to provide additional certainty that future administrations or interpretations do not confuse this application of law.

Q.3.a. Is there anything Congress should do to ensure that we don't wake up in 5 years and find that all the cryptocurrency and blockchain experts are in China or Russia?

A.3.a. Congress could pass laws that preempt State money transmission licensing obligations (as described above) and create new uniform and reasonably calibrated consumer protections in their stead. Congress could pass laws that rationalize tax treatment with respect to small transactions and capital gains (as described above). Congress could pass a law codifying the current interpretation of the SEC with respect to which technologies are and are not securities (as described above).

More generally, Congress can continue to honor and protect our constitutional freedoms by not passing laws that would seek to abridge those freedoms in return for the illusion of security. The freedom of persons to write software code related to these technologies (as guaranteed by the 1st Amendment) and the freedom from warrantless search (as guaranteed by the 4th Amendment) are America's best advantages with respect to providing a friendly home for developers building these critical technologies. These are freedoms not enjoyed by persons living in repressive regimes such as China or Russia. While new technologies will inevitably present challenges for law enforcement and financial surveillance regimes, it is imperative that we do not chip away at these freedoms and destroy the dynamism and liberty at the heart of American ingenuity. Attempts to ban the publication and distribution of

[1] See our research on State money transmission licensing here: *https://coincenter.org/entry/federal-alternative-to-state-money-transmission.*

[2] H.R. 3708, *https://www.govtrack.us/congress/bills/115/hr3708.*

cryptography-related software, for example, would backfire: these technologies exist and cannot be uninvented. They will proliferate globally whether we want them to or not. Better that America lead in these technological discoveries and pioneer a free society. This will not only preserve American ideals, it will inevitably make the stability of repressive regimes less tenable as their people adopt American tools, and clamor for American freedoms.

Q.3.b. And is there any national security risk for the United States if other countries are more welcoming, in terms of business & regulatory climate, of these new technologies?

A.3.b. Yes. The internet was the single greatest creator of jobs and prosperity in the late 20th century. America was a welcoming home for innovators building these systems and therefore continued to prosper culturally and economically. Public blockchain technologies will likely offer similar prosperity to the nations that host its pioneers. Moreover, these systems (both the internet and public blockchain networks) will continue to be essential to the security of critical infrastructure both civilian and military. Ignoring these technologies or forcing innovation overseas could prove disastrous if it leads to the further erosion of American expertise in cybersecurity and automation.

Q.4. I've recently heard from several financial institutions who have seen a growing interest in digital currency purchases. These banks and credit unions want to be able to meet customer demand while at the same time protect their customers from potential market volatility and other risks.

As the cryptocurrency market continues to grow, do you believe the Federal Government, particularly the financial regulatory agencies, should play a more active role in providing guidance to financial institutions on the purchase of cryptocurrencies?

A.4. As described earlier, a Federal alternative to State money transmission licensing would provide more cost-effective regulation of the businesses that exchange cryptocurrencies for customers. Additionally, we welcome the OCC's FinTech charter and anticipate clearer guidance on how chartered banks can safely hold cryptocurrencies on behalf of their customers.

Public Sector

Preamble: Governments across the world are exploring using blockchain technology to improve government efficiency and public services. Central banks have experimented as well.

Q.5.a. Do you believe blockchain technology is mature enough to begin implementing within the public sector?

A.5.a. We do not believe that blockchain technology is mature enough to warrant wide implementation in the public sector. Premature adoption could mean poor security for public data and it could also result in agencies adopting technological means that are rapidly made obsolete by newer developments. We've yet to see clear technological winners and losers in this space and much remains uncertain. This is a necessary stage in the evolution of new technologies. Just as the Government should not have immediately switched to email systems for messaging in the 1970s or immediately to the web for public communications in the 1990s, Government should carefully watch but generally not use public blockchain networks today. Limited pilot programs may prove the best approach.

Q.5.b. If so, what are some of the applications for blockchain in our Government that you expect could be successful?

A.5.b. Limited pilots could include using blockchain technology for identity and access control systems.

Q.6. Would you suggest the Federal Reserve consider using blockchain in its operations, as some other central banks are doing?

A.6. Blockchains are most useful when there is not a single party that everyone is willing to trust. Without this trusted party to maintain a centralized ledger of transactions, blockchains present an alternative in systems where parties are mutually distrustful. Given that we are (and will likely remain) willing to trust the Federal Reserve's decisions with respect to monetary policy, there seems little reason not to also trust them to build and maintain centralized ledgers (such as FedWire) for clearing and settlement between banks. Blockchains are not efficient or necessary in such applications.

Law Enforcement benefits from a thriving crypto/blockchain industry

Preamble: Similar to the way the creation of anti-virus software was necessary to combat computer viruses obtained through the internet, new technology will be required to track and prevent crypto or blockchain-related illicit financial activity.

Q.7. What regulatory changes can Congress or the executive branch make to ensure that American companies have the best ability to develop the necessary technology and help law enforcement combat illegal activity in the crypto and blockchain space?

A.7. The best step that Congress and the executive branch can take, is allowing security researchers to do their work unfettered by ill-conceived rules and laws intended to prevent illicit finance by placing limits on fundamental technological research and development. Anti-virus software manufacturers must—by necessity—obtain, study, and even publish virus software publicly in order to develop these defenses. The same is true for persons doing research into blockchains and their illicit use. Technology inevitably leads to arms races between criminals and law enforcement. Laws that try to deny persons access to these new technologies, whether by banning their publication or otherwise limiting public access, do not benefit law enforcement, instead these ill-conceived policies benefit criminals who—by definition—have no respect for law and would therefore have a monopoly on the development and use of these tools should they be banned or made hard to obtain through law.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR REED FROM PETER VAN VALKENBURGH

Q.1.a. Ten or twenty years from now, what is the best case scenario for our economy, especially for consumers and mom-and-pop businesses, with respect to cryptocurrencies?

A.1.a. These technologies will be as generative for prosperity and freedom as the internet has been. The best case scenario is that good policies encourage innovators to build public blockchain technology here and that America is able to reap the job growth and cultivate the security expertise inherent in those efforts.

Q.1.b. What is the worst case scenario?

A.1.b. The worse case is for these developers to be forced overseas through bad policy.

Q.1.c. What should we be doing now at the Federal level to drive toward the best case scenario?

A.1.c. Congress could pass laws that preempt State money transmission licensing obligations and create new uniform and reasonably calibrated consumer protections in their stead.[1] Congress could pass laws that rationalize tax treatment with respect to small transactions and capital gains.[2] Congress could pass a law codifying the current interpretation of the SEC with respect to which tokens and cryptocurrencies are and are not securities.

More generally, Congress can continue to honor and protect our constitutional freedoms by not passing laws that would seek to abridge those freedoms in return for the illusion of security. The freedom of persons to write software code related to these technologies (as guaranteed by the 1st Amendment) and the freedom from warrantless search (as guaranteed by the 4th Amendment) are America's best advantages with respect to providing a friendly home for developers building these critical technologies. These are freedoms not enjoyed by persons living in repressive regimes such as China or Russia. While new technologies will inevitably present challenges for law enforcement and financial surveillance regimes, it is imperative that we do not chip away at these freedoms and destroy the dynamism and liberty at the heart of American ingenuity.

Attempts to ban the publication and distribution of cryptography-related software, for example, would backfire: these technologies exist and cannot be uninvented. They will proliferate globally whether we want them to or not. Better that America lead in these technological discoveries and pioneer a free society. This will not only preserve American ideals, it will inevitably make the stability of repressive regimes less tenable as their people adopt American tools, and clamor for American freedoms.

[1] See our research on State money transmission licensing here: *https://coincenter.org/entry/federal-alternative-to-state-money-transmission.*

[2] H.R. 3708, *https://www.govtrack.us/congress/bills/115/hr3708.*

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM PETER VAN VALKENBURGH

Q.1. Many have speculated that blockchain technology or decentralized computing will revolutionize every aspect of our economy.

Why haven't we seen a breakout star application using decentralized computing yet?

A.1. The internet may be a good analogy to answer this question. Development of the networking standards that would become the internet that we know today began as early as the 1960s. Email, arguably the first "killer app" was not invented until the mid-1970s. Even then, it was not in wide use until the commercial internet began to grow in the 1990s. It wasn't until 1991 that the web (which is synonymous for most with the internet) was invented, and the first web browser (Mosaic) was not released to the public until 1993. Google was founded in 1998 and Facebook in 2004. So, given that decentralized computing is as radical and experimental a departure from existing technology as the internet was when it was first being developed, it may not be surprising that in the 10 years since Bitcoin was invented we have yet to see a mainstream "killer app."

Q.2. What is the best use case you've heard of for blockchain technologies or decentralized computing and their prospects for development and launch?

A.2. The best use case is payments without the need for a third-party intermediary. This is what cryptocurrencies like Bitcoin provide today. Perhaps more exciting from a commercial vantage point is the promise they hold to make true microtransactions economically feasible for the first time.

Q.3. What led to the collapse in cryptocurrency prices this year? Did the introduction of the Bitcoin futures contract have anything to do with it?

A.3. This is beyond the scope of my expertise.

Q.4. What approaches are other countries taking toward the regulation of cryptoassets? Are they appropriate?

A.4. The Library of Congress has published a comprehensive breakdown of cryptocurrency regulation nation-by-nation, we recommend this as a resource to the Senator if he has country-specific questions.[1] Approaches by the G20 member states vary, however, application of existing Anti-money laundering controls to financial institutions dealing in cryptocurrencies, as FinCEN did in 2013, is a common approach. We do not believe that nations should "eliminate the anonymity" that cryptocurrencies may afford; to do so would harm the legitimate privacy interests and rights of citizens. Rather, we believe that states should balance the rights of their citizens to privacy against the need for law enforcement to obtain information about criminal activities. This balance has already been struck in the context of existing forms of money, like cash transactions, and mere application of these same laws to financial institutions dealing in cryptocurrency is the best path forward. FinCEN has already offered guidance explaining why existing laws

[1] *https://www.loc.gov/law/help/cryptocurrency/world-survey.php?loclr=ealrr.*

apply and all major U.S. cryptocurrency exchanges of which we are aware now comply with these data collection obligations.

Q.5. Mr. Roubini, in his testimony, describes Vitalik Buterin's "inconsistent trinity" in blockchain—that you cannot have at the same time scalability, decentralization, and security.

Q.5.a. Is that an accurate description?

A.5.a. It is not an accurate description, as Buterin has stated himself to Roubini. Firstly, what Roubini refers to as the "inconsistent trinity" or "impossible trinity" was posited by Buterin as the "scalability trilemma," and that is how computer scientists refer to the problem. This trilemma simply states that is it difficult—not impossible—to achieve decentralization, scalability, and security at the same time in a crypto network. However, it is not an either-or proposition; it's a matter of tradeoffs along a scale.

Q.5.b. Do you believe proof of work consensus is scalable?

A.5.b. It is likely that proof-of-work consensus can scale efficiently. Proof-of-work does, indeed, use large amounts of electricity (discussed in the next answer), however the number of transactions on the network does not affect the amount of energy used. Thus a Bitcoin network processing only five transactions per second would use about as much electricity as one processing thousands per second. Miner energy usage moves up or down with the amount of competition between miners, not the number of transactions being validated. Digital signature validation uses a trivial amount of computing power. A 3-year-old laptop can verify a signature in a matter of milliseconds, and the energy used would be undetectable in an electrical bill.

Why is there so much competition driving so much energy usage? Economics. Bitcoins are expensive, and every 10 minutes one miner will get 12.5 new ones. This competition is healthy because it means that the effort spent securing the network scales automatically with the value of the transaction data on the blockchain. So the more value there is riding on the Bitcoin network, because individuals value it more as reflected in the price, the more resources will rationally be devoted to the network's security. That makes for a noteworthy contrast with data secured by, say, Equifax or any other big data company where effort spent securing data scales with a corporate management team's estimation of risks and fear of liability.

This competition may get less fierce as time goes on. The reward of new bitcoins halves every 4 years until it goes effectively to zero. Miners will keep working because they can also collect fees that users of the network add to their transaction messages, but the total take-home payment for a winning miner will probably be less than it is today even if the price of a bitcoin continues to rise. Smaller rewards will mean less computing power dedicated to winning and less electricity consumed.

Q.5.c. What do you think of his argument that proof of stake results in a centralization and concentration of mining power? Does that concern you?

A.5.c. Credible estimates have concluded that a single proof-of-work-based cryptocurrency like Bitcoin consumes as much power annually as a developed nation like Ireland. And as the value of Bitcoin grows, the energy consumption is estimated to grow even greater. And that's just for a single of the many cryptocurrencies that rely on a proof-of-work consensus mechanism.

Q.6. In light of last week's report from the UN's Panel on Climate Change that the world has at most a decade to comprehensively address climate change, shouldn't all cryptocurrency efforts be focused on less energy intensive, proof-of-stake-based cryptocurrencies?

A.6. Whether cryptocurrencies are contributing to climate change is not exclusively a question about the consensus mechanism that they use. Perhaps more important is what kind of energy they use.

Energy use is not bad in and of itself. It is greenhouses gases that are bad, but it's not a given that Bitcoin will, on net, worsen greenhouse emissions in the long run. In fact, if Bitcoin mining becomes the dominant driver of energy consumption on the planet, then that could be a good thing for the environment. Just as the consumer electronics revolution drove the massive computing efficiencies known as Moore's law; the Bitcoin revolution could drive a similar explosion of innovation in clean efficient energy.

Aluminum smelting consumes about 3 percent of the entire global supply of energy, yet we don't read articles raising the alarm on unibody MacBook Pros like we see about Bitcoin. Smelting isn't often thought of as a problem because heavy industry drives electricity efficiency. Why? Because heavy industry is a big consumer, so they're always looking for the cheapest possible source of electricity.

Heavy industry can generally be based anywhere, and electrical costs tend to be a large percentage of their total costs. Electricity is 40–45 percent of costs to chemicals manufacturing (like chlorine production) and a whopping 30–50 percent of costs to steel and aluminum smelting. That means that heavy industry will base itself where costs are lower, and that will tend to be wherever electricity is affordable because its production is more efficient. Demand drives supply and thus rewards those who develop cheaper modes of electricity generation. Lately that has roundly been a green affair. The cheapest electricity on the planet is now wind and solar energy. Geothermal and hydroelectric are also top contenders and don't have to deal with storage issues.

However, electricity costs may not always be top of mind for your typical heavy industry proprietor. They may put up with expensive, dirty energy if other costs drive their decisionmaking. Industries also like to be where their customers are, where it is cheap to ship material inputs like metal, and where governments grant them subsidies in order to encourage industrial growth.

But electricity costs matter even more to a Bitcoin miner than typical heavy industry. Electricity costs can be 30–70 percent of their total costs of operation. Also, Bitcoin miners don't need to worry about the geography of their customers or materials shipping routes. Bitcoins are digital, they have only two inputs (electricity and hardware) and network latency is trivial as compared with a truck full of steel. One miner moved an entire GPU farm across the United States because of cheap hydroelectric power in the Pacific

Northwest and, in his words, "it's worth it!" That's also why we see miners in Iceland or other places with excess capacity. Aside from beautiful vistas you can find abundant geothermal and hydraulic power in the land of volcanoes and waterfalls.

If Bitcoin mining really does begin to consume vast quantities of the global electricity supply it will, it follows, spur massive growth in efficient electricity production—*i.e.,* the green energy revolution. Moore's Law was partially a story about incredible advances in materials science, but it was also a story about incredible demand for computing that drove those advances and made semiconductor research and development profitable. If you want to see a Moore's-Law-like revolution in energy, then you should be rooting for, and not against, Bitcoin. The fact is that the Bitcoin network, right now, is providing a $200,000 bounty every 10 minutes (the mining reward) to the person who can find the cheapest energy on the planet. Got cheap green power? Bitcoin could make building more of it well worth your time.

Q.7. I've heard a lot about how a lack of a clear regulatory framework for cryptocurrencies, particularly regarding the status of whether or not a token is a security, is hindering innovation.

Q.7.a. What would be the effect in the cryptocurrency industry of the SEC setting out clear guidelines for determining whether or not a crypto asset is a security?

A.7.a. Lack of clarity has led high-quality entrepreneurs and investors to avoid risking time and capital on otherwise promising novel projects and business models. It has also allowed scammers to pretend the securities laws don't apply to the schemes they are pedaling. Greater clarity would allow investors and entrepreneurs to come safely off the sidelines, and would make clear that certain schemes are frauds. That said, the SEC has done an admirable job, in a relatively short period of time, of providing much of the clarity that innovators have sought.

Q.7.b. Do you think Congress should take action?

A.7.b. The SEC has been slowly, but surely, providing the needed clarity by explaining how it interprets the securities law. In particular, see a speech given in June by the Director of the SEC's Division of Corporation Finance, William Hinman.[2] There are still certain questions that remain open, and to the extent the SEC does not answer them it may be appropriate for Congress to do so, but there's no reason to think the SEC won't continue to provide further clarity.

Q.7.c. What would you propose?

A.7.c. At this point, to take a wait-and-see approach. That said, the guidance contained in the Hinman speech was just that—guidance—and the securities laws could be interpreted differently by a future Commission. It might be useful for Congress to codify the principles outline in the Hinman speech.

[2] *https://www.sec.gov/news/speech/speech-hinman-061418.*

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM PETER VAN VALKENBURGH [1]

Q.1. If a State were to use a stable Blockchain token as a store of value, would that be considered coinage?

A.1. The Constitution permits Congress to coin money in Article 1, Section 9 and denies States the power to coin or to print their own money in Article 1, Section 10. This is called the coinage clause. If a State merely used an existing blockchain token or cryptocurrency for payments or investment purposes, this would not, we believe, be coinage. If on the other hand a State decided to create and issue its own Blockchain token, then the State may well be coining money, contravening the constitution.

Q.2. What is the best way to crack down on the use of cryptocurrencies to finance illegal transactions dealing with drug and sex trafficking?

A.2. Applying existing Bank Secrecy Act recordkeeping and reporting requirements to financial institutions even when those institutions deal in cryptocurrencies for their customers is the best way to crack down on the use of these tools for illegal transactions. FinCEN made these obligations clear to businesses holding and transmitting cryptocurrencies in its 2013 Guidance and since then all major U.S. cryptocurrency exchanges of which we are aware now comply with the Bank Secrecy Act. The data provided by these regulated exchanges to FinCEN and law enforcement is essential to identifying illicit uses of the technology.

Q.3. What are G20 member states doing to regulate cryptocurrencies and eliminate the anonymity they supposedly afford?

A.3. The Library of Congress has published a comprehensive breakdown of cryptocurrency regulation nation-by-nation, we recommend this as a resource to the Senator if she has country-specific questions.[2] Approaches by the G20 member states vary, however, application of existing anti-money laundering controls to financial institutions dealing in cryptocurrencies, as FinCEN did in 2013, is a common approach. We do not believe that nations should "eliminate the anonymity" that cryptocurrencies may afford; to do so would harm the legitimate privacy interests and rights of citizens. Rather, we believe that states should balance the rights of their citizens to privacy against the need for law enforcement to obtain information about criminal activities. This balance has already been struck in the context of existing forms of money, like cash transactions, and mere application of these same laws to financial institutions dealing in cryptocurrency is the best path forward. FinCEN has already offered guidance explaining why existing laws apply and all major U.S. cryptocurrency exchanges of which we are aware now comply with these data collection obligations.

[1] Peter is Director of Research at Coin Center, the leading independent nonprofit research and advocacy group focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. This testimony is based largely on a report published by Coin Center. See Peter Van Valkenburgh, "Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet" Coin Center (2016) *https://coincenter.org/entry/open-matters.*

[2] *https://www.loc.gov/law/help/cryptocurrency/world-survey.php?loclr=ealrr.*

Q.4. Do you think bank customers should be able to buy cryptocurrency from their bank accounts without worrying that their bank account could be closed if they do?

A.4. Yes. If customers are unable to buy cryptocurrency though regulated financial institutions they will be more likely to seek cryptocurrency through unregulated channels, *e.g.,* face-to-face trading for cash. This would decrease the amount of information available to law enforcement investigating illicit transactions.

Q.5. Should cryptocurrency customers have their cryptocurrency purchases taxed? Such as sales tax, capital gains, *etc.?*

A.5. State sales tax is generally only imposed on purchases of tangible personal property and not on purchases of intangible property except for State-specified digital goods. See, for example, TAM—2015–1(R)—Issued July 28, 2015 by the New Jersey Tax Authority.[3] Cryptocurrency sold as an investment should be taxed as a capital gain and the IRS has clearly articulated this policy.[4] We believe there should be an exemption from capital gains taxation for small sales of cryptocurrency made for retail purposes, *e.g.,* when someone uses Bitcoin to buy a cup of coffee. This would mirror an exemption from capital gains taxation for purchases made in foreign currency, *e.g.,* when someone buys a baguette with euros they purchased in advance of a trip to Europe. A bill has been introduced in the House that would create this exemption.[5]

Q.6. Should initial coin offerings be regulated as securities, commodities, or currencies? Are they legitimate investments?

A.6. If an initial coin offering meets the existing test used by the SEC to determine whether an offering should be registered as a security then is should be regulated as such. This test, known as the Howey test, is met when a purchaser invests her money in a common enterprise with an expectation of profits dependent on the promised efforts of the ICO promoter or some other third party. Tokens traveling on a blockchain that is functional and decentralized (rather than merely a hypothetical future blockchain being promised by an ICO issuer) are not securities and should be regulated as commodities and as currencies if they are used as currency substitutes. While several ICOs have been fraudulent; many have also been legitimate investments in new technologies.

Q.7. Should cryptocurrencies have the same investor protections, the same rules against market manipulation and market fraud? Should they have adequate disclosures and investor protections? The same as bonds and stocks have?

A.7. Cryptocurrency offerings that qualify as securities as described above should have identical investor protections as traditional securities including adequate disclosures. This is the official policy of the SEC at present. Cryptocurrencies that are not securities are commodities and the CFTC has authority to police these cryptocurrency spot-markets where there is evidence of fraud and manipulation.

[3] *https://www.state.nj.us/treasury/taxation/pdf/pubs/tams/tam-2015-1.pdf.*
[4] Notice 2014–21 *https://www.irs.gov/pub/irs-drop/n-14-21.pdf.*
[5] H.R. 3708, *https://www.govtrack.us/congress/bills/115/hr3708.*

The Securities and Exchange Commission, the Commodities Futures Trading Commission and the Financial Crimes Enforcement Network are all underfunded. Monitoring these constant new cryptocurrencies is putting a further strain on their resources.

Q.8. Please provide, if any, letters to legislators or statements from crypto firms seeking appropriations for regulators so they can better monitor these investments.

A.8. Apologies, but we are aware of no such letters. Coin Center is not an industry association; we are a nonprofit research and advocacy organization focused on educating members of the Government on the subject of public blockchain technologies.

Q.9. What funding level for these agencies would virtual currencies and Blockchain firms support to ensure consumer and investor protections?

A.9. We do not have an opinion on this matter.

Q.10. Last summer, Forbes and the New York Times published a story about hackers stealing mobile phone numbers. Hackers stole phone numbers, reset someone's password and then looted their virtual currency wallets. It looks like telephone-based security is not safe.

Q.10.a. Can you describe steps owners of cryptocurrencies should do to prevent these thefts? What about the exchanges themselves? And the phone companies? And Federal and State agencies?

A.10.a. Phone numbers have been used as a second factor for 2-factor-authentication at many cryptocurrency exchanges. This means that the customer must remember and enter a password to login but she must also repeat a unique and ever-changing code that is sent to her by text message. It is true that hackers have convinced phone companies to assign numbers to the hacker's mobile phones in order to fraudulently obtain this second factor for log-in. It is true that some hackers have succeeded in stealing funds with this approach. Users should not rely on phone numbers for 2-factor-authentication. They should use device-specific tools like Google Authenticator instead. These tools cannot be reassigned to other devices by phone companies. Federal and State agencies should ensure that phone companies do not reassign phone numbers of their customers without robust proof that the request is coming from the customer themselves and not from a hacker.

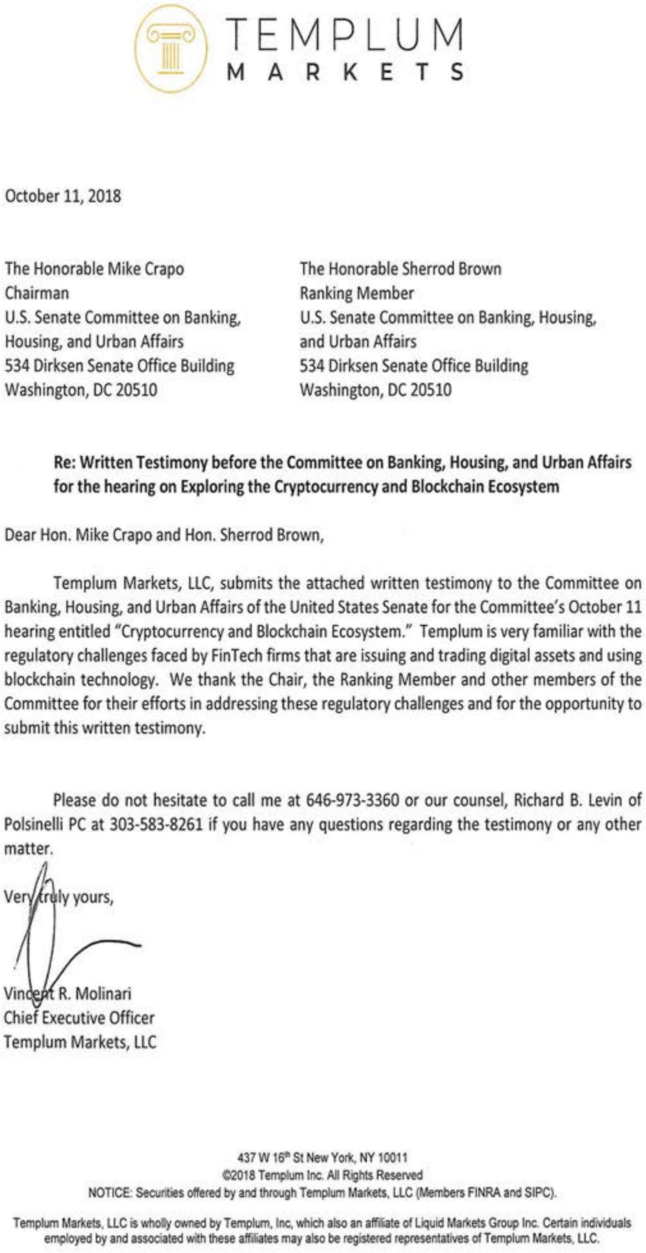
Q.11. How can we either avoid mobile phone hacks or tell people that doing financial business on a mobile phone could open you up to theft?

A.11. Nothing about mobile phones makes activities performed while using them inherently vulnerable to hacking. The problem, as described above, is that the phone's number is assigned by a phone company to an individual's device and hackers can convince phone companies to improperly reassign numbers by impersonating subscribers over the phone. This vulnerability stems from centralized companies being incapable of properly securing the integrity of data and ledgers related to their customers. Longer term, public blockchain networks could provide an alternative method of storing and maintaining the integrity of user data, just as the Bitcoin blockchain secures the data relevant to all Bitcoin transfers, without relying on trusted third parties like phone companies.

Q.12. In your testimony, you mentioned women from an African nation who were paid in bitcoin to retain their earnings instead of being forced to give their income to their husbands. How were the women able to spend their bitcoins? On what goods and services? How were those goods and services priced? What exchange fees were charged for transactions?

A.12. The woman I mentioned is Roya Mahboob and she is from Afghanistan. The primary use of Bitcoin in her story is as a store of value for women, as an alternative to savings accounts, which banks will not offer women, or cash which will often be stolen if stored in the home. As such, I am not aware of any details about spending activities. You can read more about Mahboob's story here: *https://www.ibtimes.com/afghan-tech-entrepreneur-uses-bitcoin-empower-women-2575881.*

Additional Material Supplied for the Record



TEMPLUM
MARKETS

October 11, 2018

The Honorable Mike Crapo
Chairman
U.S. Senate Committee on Banking,
Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
U.S. Senate Committee on Banking, Housing,
and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510

Re: Written Testimony before the Committee on Banking, Housing, and Urban Affairs for the hearing on Exploring the Cryptocurrency and Blockchain Ecosystem

Dear Hon. Mike Crapo and Hon. Sherrod Brown,

Templum Markets, LLC, submits the attached written testimony to the Committee on Banking, Housing, and Urban Affairs of the United States Senate for the Committee's October 11 hearing entitled "Cryptocurrency and Blockchain Ecosystem." Templum is very familiar with the regulatory challenges faced by FinTech firms that are issuing and trading digital assets and using blockchain technology. We thank the Chair, the Ranking Member and other members of the Committee for their efforts in addressing these regulatory challenges and for the opportunity to submit this written testimony.

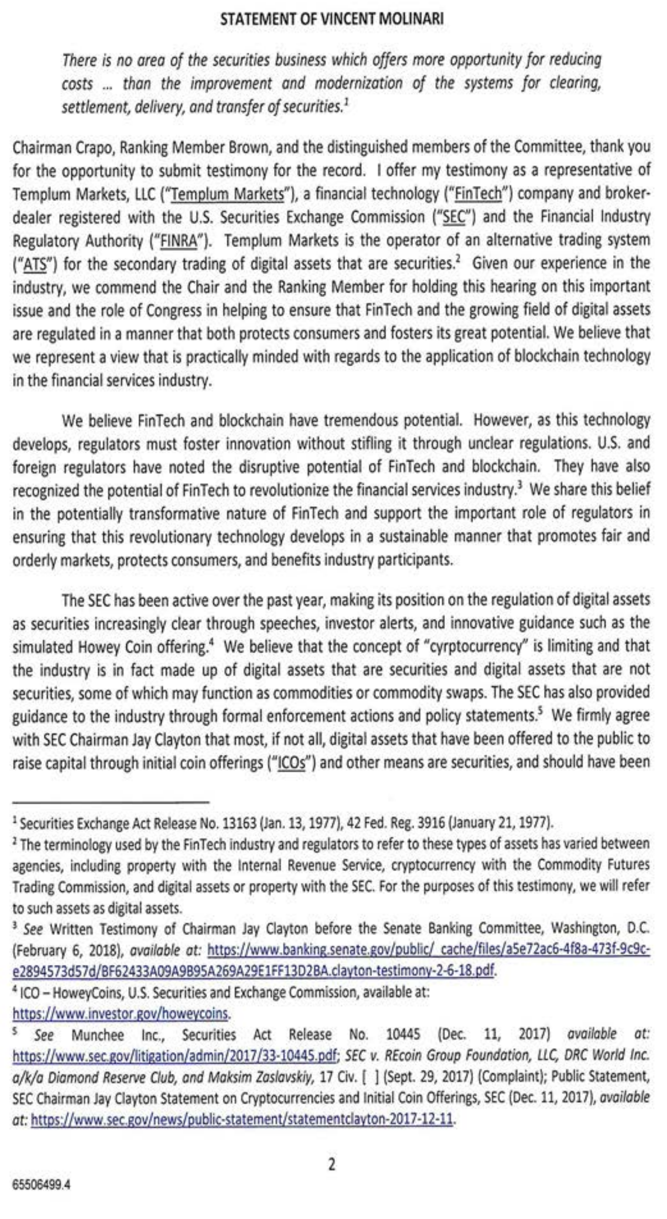
Please do not hesitate to call me at 646-973-3360 or our counsel, Richard B. Levin of Polsinelli PC at 303-583-8261 if you have any questions regarding the testimony or any other matter.

Very truly yours,

Vincent R. Molinari
Chief Executive Officer
Templum Markets, LLC

437 W 16th St New York, NY 10011
©2018 Templum Inc. All Rights Reserved
NOTICE: Securities offered by and through Templum Markets, LLC (Members FINRA and SIPC).

Templum Markets, LLC is wholly owned by Templum, Inc, which also an affiliate of Liquid Markets Group Inc. Certain individuals employed by and associated with these affiliates may also be registered representatives of Templum Markets, LLC.



STATEMENT OF VINCENT MOLINARI

> *There is no area of the securities business which offers more opportunity for reducing costs ... than the improvement and modernization of the systems for clearing, settlement, delivery, and transfer of securities.*[1]

Chairman Crapo, Ranking Member Brown, and the distinguished members of the Committee, thank you for the opportunity to submit testimony for the record. I offer my testimony as a representative of Templum Markets, LLC ("Templum Markets"), a financial technology ("FinTech") company and broker-dealer registered with the U.S. Securities Exchange Commission ("SEC") and the Financial Industry Regulatory Authority ("FINRA"). Templum Markets is the operator of an alternative trading system ("ATS") for the secondary trading of digital assets that are securities.[2] Given our experience in the industry, we commend the Chair and the Ranking Member for holding this hearing on this important issue and the role of Congress in helping to ensure that FinTech and the growing field of digital assets are regulated in a manner that both protects consumers and fosters its great potential. We believe that we represent a view that is practically minded with regards to the application of blockchain technology in the financial services industry.

We believe FinTech and blockchain have tremendous potential. However, as this technology develops, regulators must foster innovation without stifling it through unclear regulations. U.S. and foreign regulators have noted the disruptive potential of FinTech and blockchain. They have also recognized the potential of FinTech to revolutionize the financial services industry.[3] We share this belief in the potentially transformative nature of FinTech and support the important role of regulators in ensuring that this revolutionary technology develops in a sustainable manner that promotes fair and orderly markets, protects consumers, and benefits industry participants.

The SEC has been active over the past year, making its position on the regulation of digital assets as securities increasingly clear through speeches, investor alerts, and innovative guidance such as the simulated Howey Coin offering.[4] We believe that the concept of "cyrptocurrency" is limiting and that the industry is in fact made up of digital assets that are securities and digital assets that are not securities, some of which may function as commodities or commodity swaps. The SEC has also provided guidance to the industry through formal enforcement actions and policy statements.[5] We firmly agree with SEC Chairman Jay Clayton that most, if not all, digital assets that have been offered to the public to raise capital through initial coin offerings ("ICOs") and other means are securities, and should have been

[1] Securities Exchange Act Release No. 13163 (Jan. 13, 1977), 42 Fed. Reg. 3916 (January 21, 1977).

[2] The terminology used by the FinTech industry and regulators to refer to these types of assets has varied between agencies, including property with the Internal Revenue Service, cryptocurrency with the Commodity Futures Trading Commission, and digital assets or property with the SEC. For the purposes of this testimony, we will refer to such assets as digital assets.

[3] *See* Written Testimony of Chairman Jay Clayton before the Senate Banking Committee, Washington, D.C. (February 6, 2018), *available at:* https://www.banking.senate.gov/public/_cache/files/a5e72ac6-4f8a-473f-9c9c-e2894573d57d/BF62433A09A9B95A269A29E1FF13D2BA.clayton-testimony-2-6-18.pdf.

[4] ICO – HoweyCoins, U.S. Securities and Exchange Commission, available at: https://www.investor.gov/howeycoins.

[5] *See* Munchee Inc., Securities Act Release No. 10445 (Dec. 11, 2017) *available at:* https://www.sec.gov/litigation/admin/2017/33-10445.pdf; *SEC v. REcoin Group Foundation, LLC, DRC World Inc. a/k/a Diamond Reserve Club, and Maksim Zaslavskiy*, 17 Civ. [ ] (Sept. 29, 2017) (Complaint); Public Statement, SEC Chairman Jay Clayton Statement on Cryptocurrencies and Initial Coin Offerings, SEC (Dec. 11, 2017), *available at:* https://www.sec.gov/news/public-statement/statementclayton-2017-12-11.

offered pursuant to a registration with the SEC or an exemption from registration. We also appreciate that other digital assets that are not used to raise capital may be commodities or commodities swaps, subject to regulation by the Commodity Futures Trading Commission ("CFTC"). While we believe the existing laws can be applied to the regulation of blockchain technology and digital assets, we believe there is a need to modernize the securities laws, many of which were enacted by Congress in the 1930s and 1940s, to keep pace with these new technologies and to not stifle innovation. We commend the work of the SEC and CFTC to support the industry to date, including in particular the CFTC's establishment of LabCFTC, but we believe that there is more work to be done.

As Congress and the SEC consider how to regulate FinTech, we believe digital assets used to raise capital should be regulated as securities. The focus of this testimony will be with regards to the SEC's regulation of digital assets that are securities, as this is where the expertise of our firm lies. We believe such an approach will promote the development of these innovative financial products and their trading in an efficient manner, as well as market integrity. The regulation of digital assets as securities raises a number of issues including, the clearance, settlement and custody of digital assets, and the future role of transfer agents.

A. The Securities Laws Need to be Amended to Address the Regulation of Digital Assets.

The SEC's duties are to: protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.[6] The trading of digital assets has spread beyond the developers of the digital assets to large financial institutions that see the value of blockchain technology. Developing a tailored regulatory framework for digital assets would not only help to protect investors, but would help to promote market integrity, capital formation, and the protection of the investing public.

There are several specific parts of the securities laws that need to be amended to address the development of blockchain technology and digital assets and to protect investors, maintain fair and orderly markets, and to facilitate capital formation. From 1934 through 1975, trading, clearance and settlement of securities in the United States was governed by the Securities Act of 1933 (the "Securities Act"), and the Securities Exchange Act of 1934 (the "Exchange Act"). The clearance and settlement of trades was governed by state laws. It was not until the late 1960s that the SEC began focusing on how securities transactions were cleared and settled. The SEC has provided important informal guidance regarding the trading of digital assets, and in particular when a digital asset may be deemed to be a security, but the agency has not provided clear guidance on how to treat these assets post-trade. We have been an active voice in encouraging more formal regulation of FinTech, as evidenced by our March 13, 2017 petition for rulemaking to the SEC requesting regulation of digital assets of securities.[7] In addition to formal rulemaking regarding digital assets as securities, we believe that the SEC must address how digital assets are regulated once a trade occurs.

B. The Paperwork Crisis

In the late 1960s and early 1970s, securities markets in the United States experienced a back-office crisis (the "Paperwork Crisis") caused by increasing volumes and back-office inefficiencies in

[6] Michael S. Piwowar, Acting Chairman, SEC, Remarks at the "SEC Speaks" Conference 2017: Remembenng the Forgotten Investor (Feb. 24, 2017), available at: https://www.sec.gov/news/speech/piwowar-remembering-theforgotten-investor.html.

[7] See Petition for Rulemaking (Mar. 13, 2017), available at: https://www.sec.gov/rules/petitions/2017/petn4-710.pdf. At the time this petition was published, Templum Markets operated as Ouisa Capital, LLC.

processing securities transactions.[8] During the Paperwork Crisis, a brokerage firm used approximately 33 different documents to execute and record a single securities transaction.[9] These paper-based transactions slowed processing to the point where exchanges shortened the trading day to alleviate back-office delays. Clerical personnel at firms were working day and night to process transactions.[10] As the mounds of paper grew, so did the number of errors in handling and recording transactions.[11]

The confusion and delays in the back offices of brokers and dealers were magnified by inadequate clearance and settlement facilities, particularly in the over-the-counter market.[12] Systems designed for the three million share days of 1960 proved incapable of dealing with astonishing volume of thirteen million share days around the end of the decade. Operational deficiencies caused fail rates and customer complaints to soar. Losses in 1967–1968 caused an unprecedented number of broker-dealer firm failures.[13] Approximately 160 New York Stock Exchange ("NYSE") member firms went out of business while others either merged or liquidated.[14]

By the early 1970s, Congress examined the back-office crisis and asked the SEC to: (1) compile a list of unsafe and unsound practices employed by brokers and dealers in conducting their business, (2) report to Congress on steps being taken to eliminate these practices, and (3) recommend additional legislation that might be needed to eliminate these unsafe and unsound practices.

After extensive studies and hearings, Congress agreed that a fundamental weakness in the U.S. clearance and settlement system was the absence of a mechanism to give direction to, and ensure cooperation and coordination among, the entities engaged in securities processing – clearing corporations, securities depositories, transfer agents, and issuers.[15] Industry practice combined with a lack of uniformity had failed to effectively support transaction processing in the U.S., and legislation soon followed.[16]

C. Securities Act Amendments

In 1975, Congress enacted amendments to the Exchange Act finding that: (i) *the prompt and accurate clearance and settlement of securities transactions is necessary for the protection of investors*; (ii) inefficiency imposes unnecessary costs on investors and intermediaries; (iii) new data processing and communication techniques present opportunities for more efficient, effective, and safe clearing procedures; and (iv) linking of clearance and settlement facilities, and the development of uniform standards and procedures, would reduce unnecessary costs and increase investor and intermediary protection.[17]

[8] Bergmann, L., 2004. Speech: International Securities Settlement Conference – "The U.S. view of the role of regulation in market efficiency" ("Bergmann"). Available at https://www.sec.gov/news/speech/spch021004leb.htm.

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Supra* at note 6.

[16] *Supra* at note 13.

[17] 15 U.S.C. § 78q-1(a)(1)(A)-(D).

The Securities Acts Amendments of 1975 (the "Securities Acts Amendments"), made sweeping changes to the federal securities laws, established the national market system and the national clearance and settlement system as they exist today.[18] Congress directed the SEC to, among other things: (i) facilitate the establishment of a national system for the prompt and accurate clearance and settlement of transactions in securities and (ii) end the physical movement of securities certificates in connection with the settlement among brokers and dealers of transactions in securities.

Two basic themes recur throughout the legislative history of the securities processing provisions of the Securities Acts Amendments: (i) prevent another paperwork crisis in the securities industry and (ii) establish a safe, efficient, and modern national clearing and settlement system. Section 17A of the Exchange Act gave the SEC the authority to facilitate: (i) the establishment of a national system for prompt and accurate clearance and settlement in securities and (ii) linked or coordinated facilities for clearance and settlement of related financial products. Congress directed the SEC in 1975 to facilitate the establishment of a national system for the prompt and accurate clearance and settlement of securities transactions when it added Section 17A to the Exchange Act as part of the Securities Acts Amendments. At the time of the adoption of the Securities Acts Amendments, the Senate Committee on Banking, Housing and Urban Affairs stated the "banking and security industries must move quickly toward the establishment of a fully integrated national system for the prompt and accurate processing and settlement of securities transactions".

A key component of the SEC's supervision of the securities clearance and settlement system is its authority to regulate clearing agencies. Before performing clearing agency functions, including trade comparison, netting, matching, and settlement activities, intermediaries must either register with the SEC or apply for an exemption from registration. The SEC's ability to achieve these goals and its supervision of securities clearance and settlement systems is based on the regulation of registered clearing agencies.

While blockchain technology was not available in 1975, many technologists believe the technology could help the financial services industry accomplish many of the goals of the Securities Acts Amendments. The question for Congress and the industry will be how such technologies should be regulated by the SEC.

D. Clearing Agencies

Clearing agencies are self-regulatory organizations that are required to register with the SEC. There are two types of clearing agencies: clearing corporations and depositories. Clearing corporations compare member transactions (or report to members the results of exchange comparison operations), clear those trades and prepare instructions for automated settlement of those trades, and often act as intermediaries in making those settlements. Clearing corporations provide several essential services to the market, including comparing and confirming trade data submitted by participants (or reporting to participants the results of trade comparisons submitted by the exchanges), acting as the common counterparty and guaranteeing the completion of the trade if either side defaults or goes out of business, and preparing instructions for their participants regarding their settlement obligations. Clearing corporations generally instruct depositories to make securities deliveries that result from settlement of securities transactions.

[18] 15 U.S.C. §78q-1(a)(2).

A blockchain technology platform could be required to register as a clearing corporation if it compares the trades of users of the platform, clears the trades, and prepares instructions for automated settlement of the trades. The platform could also be required to register as a clearing corporation if the platform acts as the common counterparty and guarantees the completion of trades. We encourage the SEC to clearly define when a blockchain technology platform must register as a clearing corporation and to define how blockchain technology may be used by such firms.

E. Transfer Agents

Blockchain and digital assets represent a fundamental change in the financial services industry and hold the potential to make traditional aspects of the industry obsolete. One area of the securities laws that can be improved through the introduction of blockchain is the role of transfer agents. Traditionally transfer agents perform functions such as: countersigning securities upon issuance, monitoring the issuance of securities with a view to preventing unauthorized issuance, a function commonly performed by a person called a registrar, registering the transfer of securities, exchanging or converting securities, or transferring record ownership of securities by bookkeeping entry without physical issuance of securities certificates.[19] Transfer agents record changes of ownership, maintain the issuer's security holder records, cancel and issue certificates, and distribute dividends. Because transfer agents stand between issuing companies and security holders, efficient transfer agent operations are critical to the successful completion of secondary trades. Section 17A(c) of the Exchange Act requires that transfer agents be registered with the SEC, or if the transfer agent is a bank, with a bank regulatory agency.

A blockchain technology platform could be required to register as a transfer agent if it monitors the issuance of securities or registers the transfers of securities. While it is unlikely a blockchain technology platform would countersign securities, platforms operating their own blockchain to track the issuance and trading of digital assets could be deemed to be monitoring the issuance of securities with a view of preventing unauthorized issuance (i.e., a registrar, registering the transferring of such securities). Other blockchain platforms could be deemed to be registering the transfer of securities, exchanging or converting securities, or transferring record ownership of securities by a bookkeeping or ledger entry without physical issuance of securities certifications.

The SEC released a concept release regarding transfer agents in 2015, noting the potential value of blockchain technology in streamlining the industry.[20] We encourage Congress to instruct the SEC to provide clear guidance to the industry as to when a blockchain technology platform must register as a transfer agent and to provide guidance to issuers of digital assets as to when they must use a transfer agent.

F. Clearinghouses

Like transfer agents, clearinghouses perform a valuable function in the financial services industry that is being impacted by the advent of blockchain technology. Generally, clearinghouses such as the Depository Trust and Clearing Corporation ("DTCC") are relied upon in the trading of registered securities to stand between clearing firms in ensuring that a transaction is properly settled. The securities that may be made eligible for DTCC's book-entry delivery, settlement and depository services are those that have been issued in a transaction that: has been registered with the SEC pursuant to the

[19] Securities Exchange Act of 1934 Section 3(a)(25).

[20] Securities Exchange Act Release No. 76743 (Dec. 22, 2015), 80 Fed. Reg. 81948 (Dec. 31, 2015). Available at www.sec.gov/rules/concept/2015/34-76743.pdf.

Securities Act; was exempt from registration pursuant to a Securities Act exemption that does not involve (or, at the time of the request for eligibility, no longer involves) transfer or ownership restrictions; or permits resale of the securities pursuant to Rule 144A or Regulation S, and, in all cases, such securities otherwise meet DTCC's eligibility criteria.

A wide range of security types may be made eligible for DTCC's services in accordance with the DTCC Rules. These include, but are not limited to, equities, warrants, rights, corporate debt and notes, municipal bonds, government securities, asset-backed securities, collateralized mortgage obligations, equity and debt derivatives, variable-rate demand obligations, money market instruments (e.g., commercial paper, bankers' acceptances, institutional certificates of deposit, short-term bank notes, discount notes and certain medium-term notes), American/global depositary receipts, shares of closed end funds, retail certificates of deposits, unit investment trust certificates, shares of exchange traded funds and insured custodial receipts.

Currently, digital assets that are not registered with the SEC are ineligible for book entry delivery through the DTCC. Blockchain technology, however, allows parties to transact directly with each other through a network by leveraging its distributed nature, largely eliminating the need for traditional clearinghouses. We believe Congress should encourage the SEC to evaluate the use of blockchain technology for securities that are not DTCC eligible. Leveraging blockchain will allow parties to streamline transactions and reduce friction, while promoting market efficiency. Clearinghouses are able to process transactions in registered securities that are listed on an exchange; they are not currently able to process transactions in digital assets that are securities that are not DTCC eligible. We encourage the SEC and the DTCC to explore how digital assets that are securities could be DTCC eligible securities.

G. Custody

Section 15(c)(3) of the Exchange Act and Rule 15c3-3 (the "Customer Protection Rule"), are designed to protect customer funds with two main requirements: possession or control of securities, and reserve formula. The requirements have the objectives of establishing guidelines to calculate customer assets to be segregated, methods to segregate and practices to prevent broker-dealers from using segregated customer assets to finance their proprietary activities, satisfying deliveries and covering customer short transactions. Specifically, the rule requires that customer funds involved in an applicable securities transaction be held at a bank as defined in the Exchange Act. The Rule also requires a broker-dealer to maintain physical possession or control over customers' fully paid and excess margin securities. Physical possession or control generally means that the broker-dealer must hold securities in one of several locations specified in the rule and that they be held free of liens or any other interest that could be exercised by a third-party to secure an obligation of the broker-dealer.

The SEC has also addressed the issue of custody in the context of registered investment advisers under the Investment Advisers Act of 1940 (the "Advisers Act"). Under the Advisers Act, the SEC has stated that ***no qualified custodian is required for uncertificated or certificated private shares***. While the SEC has provided guidance to registered investment advisers, it has not provided guidance to broker-dealers. The Customer Protection Rule serves a laudable goals, under both the Exchange Act and Advisers Act. However, the application of the rule is unclear in a world of digital assets that are securities and blockchain technology. It is unclear if digital assets that are unregistered securities must be held in compliance with the Customer Protection Rule and any applicable custody rule.

We believe blockchain technology has the potential to reshape how banks act as custodians, particularly with respect to digital assets that are securities. Blockchain has the ability to hold digital assets that are securities and record their transfer. We encourage Congress to instruct the SEC to examine the custody rule and the Customer Protection Rule in light of blockchain technology. By allowing issuers or trading platforms to use blockchain technology in lieu of banks as custodians, the SEC could significantly streamline securities trading and reduce transaction costs, producing savings for investors. Such efficiencies created by blockchain have great potential when used on a large scale. To facilitate this, the SEC needs to modernize its traditional rules and regulations to embrace blockchain technology.

H. Recommendations

To support the goals described above, we recommend that Congress support the following initiatives and rulemaking: (1) The SEC and CFTC should publish concept releases regarding the regulation of digital assets. The concept release should be published in compliance with the provisions of the Administrative Procedure Act, in particular providing the public with a period of notice and comment. (2) We encourage Congress to instruct the SEC to provide clear guidance to the industry as to when a blockchain technology platform must register as a transfer agent and to provide guidance to issuers of digital assets as to when they must use a transfer agent. (3) The SEC should consider changes to existing regulations with regard to the clearance and settlement of transactions in order to promote market efficiency, especially in post-trade contexts.

I. Conclusion

Innovation and entrepreneurship is at the heart American economy, and blockchain technology is driving innovation in the financial services industry. We firmly believe that blockchain has the potential to revolutionize financial services. To do so, however, Congress needs to amend the securities laws to give the SEC the tools it needs to regulate blockchain technology and digital assets and how the agency regulates transfer agents, clearinghouses, and custody. Such regulation would provide needed legitimacy to the industry, support market development, and protect investors.