AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

BEYOND BITCOIN: EMERGING APPLICATIONS FOR BLOCKCHAIN TECHNOLOGY

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT &
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

FEBRUARY 14, 2018

Serial No. 115–47

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
28–934PDF WASHINGTON : 2018

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma
DANA ROHRABACHER, California
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
JIM BRIDENSTINE, Oklahoma
RANDY K. WEBER, Texas
STEPHEN KNIGHT, California
BRIAN BABIN, Texas
BARBARA COMSTOCK, Virginia
BARRY LOUDERMILK, Georgia
RALPH LEE ABRAHAM, Louisiana
DANIEL WEBSTER, Florida
JIM BANKS, Indiana
ANDY BIGGS, Arizona
ROGER W. MARSHALL, Kansas
NEAL P. DUNN, Florida
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
SUZANNE BONAMICI, Oregon
AMI BERA, California
ELIZABETH H. ESTY, Connecticut
MARC A. VEASEY, Texas
DONALD S. BEYER, JR., Virginia
JACKY ROSEN, Nevada
JERRY MCNERNEY, California
ED PERLMUTTER, Colorado
PAUL TONKO, New York
BILL FOSTER, Illinois
MARK TAKANO, California
COLLEEN HANABUSA, Hawaii
CHARLIE CRIST, Florida

SUBCOMMITTEE ON OVERSIGHT

RALPH LEE ABRAHAM, LOUISIANA, *Chair*

FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
BARRY LOUDERMILK, Georgia
ROGER W. MARSHALL, Kansas
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
LAMAR S. SMITH, Texas

DONALD S. BEYER, Jr., Virginia
JERRY MCNERNEY, California
ED PERLMUTTER, Colorado
EDDIE BERNICE JOHNSON, Texas

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. BARBARA COMSTOCK, Virginia, *Chair*

FRANK D. LUCAS, Oklahoma
RANDY HULTGREN, Illinois
STEPHEN KNIGHT, California
RALPH LEE ABRAHAM, Louisiana
DANIEL WEBSTER, Florida
JIM BANKS, Indiana
ROGER W. MARSHALL, Kansas
LAMAR S. SMITH, Texas

DANIEL LIPINSKI, Illinois
ELIZABETH H. ESTY, Connecticut
JACKY ROSEN, Nevada
SUZANNE BONAMICI, Oregon
AMI BERA, California
DONALD S. BEYER, JR., Virginia
EDDIE BERNICE JOHNSON, Texas

CONTENTS

February 14, 2018

	Page
Witness List	2
Hearing Charter	3

Opening Statements

Statement by Representative Ralph Lee Abraham, Chairman, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	4
Written Statement	6
Statement by Representative Donald S. Beyer, Jr., Ranking Member, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	8
Written Statement	10
Statement by Representative Barbara Comstock, Chairwoman, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	12
Written Statement	13
Written Statement by Representative Eddie Bernice Johnson, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives	15
Written Statement by Representative Daniel Lipinski, Ranking Member, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	16

Witnesses:

Mr. Chris A. Jaikaran, Analyst in Cybersecurity Policy, Government and Finance Division, Congressional Research Service	
Oral Statement	17
Written Statement	20
Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology	
Oral Statement	31
Written Statement	33
Mr. Gennaro "Jerry" Cuomo, IBM Fellow and Vice President Blockchain Technologies, IBM Cloud	
Oral Statement	41
Written Statement	43
Mr. Frank Yiannas, Vice President of Food Safety, Walmart	
Oral Statement	52
Written Statement	54
Mr. Aaron Wright, Associate Clinical Professor and Co-Director of the Blockchain Project, Benjamin N. Cardozo School of Law	
Oral Statement	64
Written Statement	67
Discussion	74

Page

Appendix I: Additional Material for the Record

Letter submitted by Representative Representative Donald S. Beyer, Jr., Ranking Member, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives 104

BEYOND BITCOIN: EMERGING APPLICATIONS FOR BLOCKCHAIN TECHNOLOGY

WEDNESDAY, FEBRUARY 14, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to call, at 10:03 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Ralph Abraham [Chairman of the Subcommittee on Oversight] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
www.science.house.gov

Beyond Bitcoin: Emerging Applications for Blockchain Technology

Wednesday, February 14, 2017
10:00 a.m.
2318 Rayburn House Office Building

Witnesses

Mr. Chris A. Jaikaran, Analyst in Cybersecurity Policy, Government and Finance Division, Congressional Research Service

Dr. Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology

Mr. Gennaro "Jerry" Cuomo, IBM Fellow, Vice President Blockchain Technologies, IBM Cloud

Mr. Frank Yiannas, Vice President of Food Safety, Walmart

Mr. Aaron Wright, Associate Clinical Professor and Co-Director of the Blockchain Project, Benjamin N. Cardozo School of Law

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HEARING CHARTER

February 14, 2018

TO: Members, Subcommittees on Oversight and Research and Technology

FROM: Majority Staff, Committee on Science, Space, and Technology

SUBJECT: Oversight Subcommittee and Research and Technology Subcommittee joint hearing: *Beyond Bitcoin: Emerging Applications for Blockchain Technology*.

The Subcommittees on Oversight and Research and Technology will hold a joint hearing entitled *Beyond Bitcoin: Emerging Applications for Blockchain Technology* on Wednesday, February 14, 2018, at 10:00 a.m. in Room 2318 of the Rayburn House Office Building.

Hearing Purpose:

The purpose of this hearing is to explore the science of blockchain technology and its potential and emerging applications beyond cryptocurrency and financial technology. The hearing will focus on applications for blockchain technology across a broad range of industries, including cybersecurity, identity authentication and verification, supply chain risk management, and digital rights management. The hearing will also look at standards, guidelines, uses for government, and best practices that may prove necessary for the effective utilization of blockchain technology with respect to these emerging applications.

Witness List:

- **Mr. Chris A. Jaikaran**, Analyst in Cybersecurity Policy, Government and Finance Division, Congressional Research Service
- **Dr. Charles H. Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology
- **Mr. Gennaro "Jerry" Cuomo**, IBM Fellow, Vice President Blockchain Technologies, IBM Cloud
- **Mr. Frank Yiannas**, Vice President of Food Safety, Walmart
- **Mr. Aaron Wright**, Associate Clinical Professor and Co-Director of the Blockchain Project, Benjamin N. Cardozo School of Law

Staff Contact:

For questions related to the hearing, please contact Drew Colliatie or Tom Connally of the Majority Staff at 202-225-6371.

Chairman ABRAHAM. The Subcommittee on Oversight and Research and Technology will come to order.

Without objection, the Chair is authorized to declare recess of the Subcommittee at any time.

Good morning. Welcome to today's hearing entitled "Beyond Bitcoin: Emerging Applications for Blockchain Technology." I'm going to recognize myself for five minutes for an opening statement.

Again, good morning, and welcome to the panelists—I think I've met most of you—to this joint Oversight and Research and Technology Subcommittee hearing. And again, the title is "Beyond Bitcoin: Emerging Applications for Blockchain Technology."

The purpose of this hearing is to explore blockchain technology, its potential, and emerging applications beyond cryptocurrency and financial technology. Today, we will hear from government and private-sector experts about the basics of blockchain technology and the ways this emerging technology can be leveraged to improve the provision of products and services for government and industry alike.

Historically, the Science Committee has engaged in vigorous oversight of emerging forms of research and technology, especially those that stand to directly benefit business and government by ensuring their reliability, increasing their productivity, and securing systems and data.

This hearing is an opportunity to learn more about the standards, guidelines, and best practices that may be necessary to ensure the effective and appropriate implementation of blockchain technology to those emerging applications, and I look forward to hearing from the witnesses today about improving certainly our government efficiency and private-sector successes with this technology.

And while there has been much discussion throughout Congress regarding the cryptocurrencies, this hearing is not intended to discuss those directly such as Bitcoin, and the numerous reported security, regulatory, and environmental issues associated with them. And although Bitcoin and other cryptocurrencies are popular and eye-catching examples of the use of blockchain technology, we will learn today that there are many emerging applications with much potential that could eventually provide substantial benefits to businesses and taxpayers.

The Committee hopes to highlight this often underreported use of blockchain technology without getting caught up in the topic of the recently volatile and unsecure cryptocurrencies. We are also interested in the ongoing, proactive efforts and the coordination among private industries utilizing blockchain technology in different areas of their business models.

I wish to thank Mr. Cuomo for being here to represent IBM, Mr. Yiannas is representing Walmart, and we look forward to hearing about the specific actions of IBM and Walmart have taken to utilize and harness the strength of this technology, especially in the supply chain and data management domains.

Beyond an interest in the application of blockchain technology, the Science Committee will continue to address cybersecurity and how incorporation of blockchain technology could potentially bolster

private companies' and the federal government's cybersecurity weaknesses. Cybersecurity is a complex and evolving issue that affects U.S. national and economic security, and we must consider the appropriate role for blockchain technology. All departments and agencies must remain diligent in their efforts to strengthen and secure our federal systems, and our approaches to addressing cybersecurity issues must evolve to keep pace with the everchanging threats.

Bolstering the cybersecurity of federal information systems is among the Committee's top priorities, and I'm hopeful that our efforts here today will take us one step closer to achieving this objective.

Dr. Romine, we appreciate NIST being here, and thank you for the—continuing to provide the guidance on this emerging technology. I know it's an evolving and very rapidly changing field. NIST is in a unique position to provide valuable standards and guidelines for blockchain with their extensive involvement with cryptography, the mathematical tools at the heart of blockchain technology. NIST has the ability to effectively ensure current standards—that current standards are sufficient in addressing potential for blockchain technology being utilized on a broader and a more intensive scale.

And additionally, NIST can serve a useful role in providing a greater understanding of how the technology could lead to solutions that help secure data and ultimately enhance our national security, which is critical.

I look forward to the insight of our witnesses today—they will provide, which will help resolve these important questions and hopefully help us better understand the next steps that must be taken to ensure the integrity, the resilience, and the security of systems and industries that could and do benefit from the application of this technology.

[The prepared statement of Chairman Abraham follows:]

For Immediate Release
February 14, 2018

Media Contacts: Thea McDonald, Brandon VerVelde
(202) 225-6371

Statement by Chairman Ralph Abraham (R-La.)

Beyond Bitcoin: Emerging Applications for Blockchain Technology

Chairman Abraham: Good morning and welcome to today's joint Oversight and Research and Technology Subcommittee hearing, Beyond Bitcoin: Emerging Applications for Blockchain Technology.

The purpose of this hearing is to explore blockchain technology, its potential, and emerging applications beyond cryptocurrency and financial technology. Today, we will hear from government and private sector experts about the basics of blockchain technology and the ways this emerging technology can be leveraged to improve the provision of products and services for government and industry alike.

Historically, the Science Committee has engaged in vigorous oversight of emerging forms of research and technology, especially those that stand to directly benefit business and government by ensuring reliability, increasing productivity, and securing systems and data.

This hearing is an opportunity to learn more about standards, guidelines and best practices that may be necessary to ensure the effective and appropriate implementation of blockchain technology to these emerging applications. I look forward to hearing from today's witnesses about ways to improve government efficiency and private sector successes with this technology.

While there has been much discussion throughout Congress regarding cryptocurrencies, this hearing is not intended to discuss cryptocurrencies, such as Bitcoin, and the numerous reported security, regulatory and environmental issues associated with them. Although Bitcoin and other cryptocurrencies are popular and eye-catching examples of the use of blockchain technology, we will learn today that there are many emerging applications with much potential that could eventually provide substantial benefits to businesses and taxpayers. The committee hopes to highlight the often underreported uses of blockchain technology without getting caught up in the topic of the recently volatile and unsecure cryptocurrencies.

We are also interested in the ongoing, proactive efforts and coordination among private industries utilizing blockchain technology in different areas of their business models. I want to thank Mr. Cuomo for being here to represent IBM and Mr. Yiannas representing Walmart. We look forward to learning about the specific actions IBM and Walmart have taken to utilize and harness the strengths of the technology, especially in the supply chain and data management domains.

Beyond an interest in the application of blockchain technology, the Science Committee will continue to address cybersecurity and how incorporation of blockchain technology could potentially bolster private companies' and the federal government's cybersecurity weaknesses. Cybersecurity is a complex and evolving issue that affects U.S. national and economic security, and we must consider the appropriate role for blockchain technology. All departments and agencies must remain diligent in their efforts to strengthen and secure federal systems, and our approaches to addressing cybersecurity issues must evolve to keep pace with ever-changing threats. Bolstering the cybersecurity of federal information systems is among the committee's top priorities, and I am hopeful that our efforts here today will take us one step closer toward accomplishing this objective.

Dr. Romine, we appreciate the expertise of NIST and thank you for continuing to provide guidance on this emerging technology. NIST is in a unique position to provide valuable standards and guidelines for blockchain with their extensive involvement with cryptography — the mathematical tools at the heart of blockchain technology. NIST has the ability to effectively ensure current standards are sufficient in addressing potential for blockchain technology being utilized on a broader and more intensive scale. Additionally, NIST can serve a useful role in providing a greater understanding of how the technology could lead to solutions that help secure data and ultimately enhance our national security.

I look forward to the insight our witnesses today will provide, which will help us resolve these important questions and better understand the next steps that must be taken to ensure the integrity, resilience and security of systems and industry that could and do benefit from the application of this technology.

###

Chairman ABRAHAM. Next, Mr. Beyer. I now recognize the Ranking Member of the Oversight Subcommittee, the gentleman from Virginia, Mr. Beyer, for an opening statement.

Mr. BEYER. Thank you, Mr. Chairman, very much. Congratulations on your new chairmanship——

Chairman ABRAHAM. Thank you. I appreciate that.

Mr. BEYER. —of this Oversight. And I want to thank you and Chairwoman Comstock for putting on this hearing. It's a fascinating topic. I've been asking everyone I know in the last week to explain blockchain technology to me. No one can. People can spell it; that's about all. So I'm hoping that after we get finished today, you guys will also explain special relativity and quantum mechanics to the rest of the team, too.

But this really is incredibly important. I just came back from the World Economic Forum where it seemed like every other forum was about blockchain technology. So entrepreneurs, innovators, big business, small businesses, small enterprises, everyone seems to be scrambling to understand the applications of blockchain technology. And as the hearing title suggests, it seems to be quickly moved past Bitcoin and past cryptocurrencies into supply chain industry, health care, clean energy field, legal/financial markets, election infrastructure. I read a great article last week about how it could affect education in the years to come.

So this—potential blockchains offer better security, enhanced privacy, transactional transparency. But it's also obviously a disruptive technology, and so government and law enforcement agencies are trying to start to figure out the ramifications of blockchain services and applications. We know they have a difficult task ahead of them. As a nation, I believe that all of us want to ensure that these blockchain-based technologies are used appropriately, that government regulations are not disregarded or intentionally circumvented, but at the same time that they aren't burdensome, that we are encouraging innovation and broad-based applications when appropriate and advantageous.

So I'm particularly interested in hearing all that you have to say and the specific steps that you believe the U.S. Government, particularly our science-based agencies—NIST, National Science Foundation, Department of Energy, and Homeland Security—should be taking to foster innovation in this field and to help ensure that America is the hub for blockchain research development and discovery.

By the way, Chairman Abraham, I believe the Science Committee can play an important oversight role in providing a public forum to address these and many other issues, so I'm hoping that past blockchain will look at the ethical issues surrounding artificial intelligence and mimicking software where we draw the limits and regulate such technology; that we think about the security consequences of deploying autonomous vehicles, drones, and other similar technologies; what are the technical challenges and the ethical implications of implantable medical devices and brain computer interfaces; and how can we or should we keep a closer eye on the deployment of commercially owned and operated biometric and other surveillance technologies both online, in the streets, and in the retail stores across America?

This is a very fun committee to be on because we're dealing with so many things that are absolute—you know, that we wouldn't have predicted three years ago, maybe last year. So thank you very much for coming and educating us. We hope to ask intelligent questions. We hope to be a lot smarter at the end of this. Mr. Chairman, I yield back.

[The prepared statement of Mr. Beyer follows:]

OPENING STATEMENT
Ranking Member Donald S. Beyer Jr. (D-VA)
of the Subcommittee on Oversight

House Committee on Science, Space, and Technology
Subcommittee on Oversight
Subcommittee on Research and Technology
Beyond Bitcoin: Emerging Applications for Blockchain Technology
February 14, 2018

Thank you Chairman Abraham and Chairwoman Comstock.

This is a fascinating topic and I am glad we are examining the issue of blockchain technology today. Entrepreneurs, innovators, big businesses and small enterprises, all seem to be scrambling to understand possible applications of blockchain-based technologies. As the hearing title, suggests, blockchain technology has moved *beyond* cryptocurrencies into areas as diverse as the supply chain industry, healthcare, the clean energy sector, legal field, financial markets, and possibly even our election infrastructure. Blockchains have the potential to offer better security, enhanced privacy, and transactional transparency.

Blockchain appears to be a potentially disruptive technology, and government regulatory and law enforcement agencies are starting to figure out the ramifications of new blockchain-based services and applications. These agencies have a difficult task ahead of them. As a nation, I believe we want to ensure these blockchain-based technologies are used appropriately and that government regulations are not disregarded or intentionally circumvented by their use. At the same time, however, we want to encourage innovation and broad-based applications of blockchain-based technology when and where appropriate and advantageous.

I am particularly interested in hearing what specific steps our witnesses believe the U.S. government, particularly our science-based agencies including the National Science Foundation, Departments of Energy and Homeland Security, and the National Institute for Standards and Technology, should be taking to foster innovation in this field and help to ensure that America is a hub for blockchain research, development and discovery.

Chairman Abraham, I believe the Science Committee can play an important oversight role in providing a public forum to address these and other emerging technology-related issues that have broad implications for our society, our economy and our homeland security. I'm glad to see us dig into an emerging technology in such a bipartisan manner today, and think there are some other topics it might benefit us to explore as a Committee as well, including:

- What are the ethical issues surrounding emerging artificial intelligence and mimicking software, and where must we draw limits and regulate such technology?

- What are the security consequences of deploying autonomous vehicles, drones and other similar technologies on our streets and in the air?

- What are the technical challenges, security concerns and ethical implications we face from a growing list of implantable medical devices and brain-computer interfaces?

- How can we, or should we, keep a closer eye on the deployment of commercially owned and operated biometric and other surveillance technologies both online, on the streets, and in retail stores across America?

I hope that you will consider having future hearings that examine the wide-range of new and emerging technologies that are likely to affect Americans in distinct and dramatic ways. I am optimistic that our examination of blockchain-based technologies and their potential applications and implications is just the first of similar hearings the Committee will hold down the road.

I look forward to hearing from all of our witnesses today. Thank you.

I yield back my time.

Chairman ABRAHAM. Thank you, Mr. Beyer.

And I now recognize the Chair of the Research and Technology Subcommittee, Mrs. Comstock, for an opening statement.

Mrs. COMSTOCK. Thank you, Chairman Abraham, for putting together this hearing on such an important topic, and congratulations on your new position as Chairman of the Oversight Subcommittee.

Today's hearing topic is of great interest to me and my constituents in the Commonwealth of Virginia. The 10th District attracts many of the leading internet, high-tech, health and defense companies in the world, and the northern Virginia region is home to many research and technology companies on the forefront of innovation.

A recent overview by the National Institute of Standards and Technology describes blockchains as, quote, "a significant new avenue for technological advancements, enabling secure transactions without the need for a central authority," end quote. While many of my more technologically inclined constituents may grasp the cryptocurrency benefits of blockchain technology, today's hearing will provide some insights into blockchain's applications beyond cryptocurrency.

Blockchains have a myriad of applications in areas such as cybersecurity, identity authentication and verification, supply chain risk management and digital rights management, among others. These applications have potential implications and benefits for the federal government. A recent Department of Transportation report notes that there are "several proposed, ongoing, and theoretical ways of applying blockchains in government." This includes the State Department's exploration of ways to use blockchain to improve efficiency, as well as research by the Postal Service and Department of Homeland Security on how blockchains may help in the establishment of secure identity management. I am pleased to hear about such efforts.

In the previous session of Congress, the Research and Technology Subcommittee held a hearing following the many data breaches at the Office of Personnel Management. Like thousands of my constituents, I, too, received a letter from OPM informing me that my personal information may have been compromised or stolen by the criminals behind this attack. I also received a letter from the IRS on the same, and—I think I got three letters. I think I hit the trifecta on letters and information being compromised.

So I look forward to hearing more about the potential and emerging applications of blockchain technology today, particularly if the technology can help with securing people's private and sensitive information. Thank you, and I yield back.

[The prepared statement of Mrs. Comstock follows:]

For Immediate Release
February 14, 2018

Media Contacts: Thea McDonald, Brandon VerVelde
(202) 225-6371

Statement by Chairwoman Barbara Comstock (R-Va.)

Beyond Bitcoin: Emerging Applications for Blockchain Technology

Chairwoman Comstock: I would like to thank Chairman Abraham for putting together this hearing on such an important topic and congratulate him on his new position as Chairman of the Oversight Subcommittee. We will miss him on the Research and Technology Subcommittee, but I look forward to working with him in his new role and on joint ventures such as this hearing.

Today's hearing topic is of great interest to me and my constituents in the Commonwealth of Virginia.

The 10th District attracts many of the leading internet, high-tech, health and defense companies in the world, and the Northern Virginia region is home to many research and technology companies on the forefront of technological innovation.

A recent overview by the National Institute of Standards and Technology describes blockchains as "a significant new avenue for technological advancements, enabling secure transactions without the need for a central authority." While many of my more technologically inclined constituents may grasp the cryptocurrency benefits of blockchain technology, today's hearing will provide some insights into blockchain's applications beyond cryptocurrency.

Blockchains have a myriad of applications in areas such as cybersecurity, identity authentication and verification, supply chain risk management and digital rights management, among others.

These applications have potential implications and benefits for the federal government. A recent Department of Transportation report notes that there are "several proposed, ongoing and theoretical ways of applying blockchains in government." This includes the State Department's exploration of ways to use blockchain to improve efficiency, as well as research by the U.S. Postal Service and Department of Homeland Security on how blockchains may help in the establishment of secure identity management.

I am pleased to hear about such efforts. In the previous session of Congress, the Research and Technology Subcommittee held a hearing following the data breaches at the Office of Personnel Management (OPM). Like thousands of my constituents, I, too, received a letter from OPM informing me that my personal information may have been compromised or stolen by the criminals behind this attack.

I look forward to hearing more about the potential and emerging applications of blockchain technology today, particularly if the technology can help our government do a better job of securing people's private and sensitive information.

###

[The prepared statement of Ranking Member Johnson follows:]

OPENING STATEMENT
Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
Subcommittee on Oversight
Subcommittee on Research and Technology
"Beyond Bitcoin: Emerging Applications for Blockchain Technology"
February 14, 2018

Thank you Chairman Abraham.

I am glad that the Committee is holding this hearing today on the emerging applications of blockchain technology. Blockchain technology has the potential to change voting, identity verification, taxation, medical care, contracts, shipping, shopping, and many other facets of life. We on the Science Committee need to better understand this important technology and proactively address policies to spur its responsible development here in the United States. I am happy that NIST, the National Institute of Standards and Technology, is here to discuss its work related to blockchain technology, particularly its work in the development of national and international standards.

China, Japan, the United Arab Emirates, and the European Union have all taken blockchain technology quite seriously. They have all invested in research and initiated pilot programs using the technology. The European Union has begun to examine some of the potential needs for blockchain regulation, while trying not to stifle innovation. The international competition has begun, and we in Congress must do our part to make sure that the United States remains the center of blockchain innovation and use.

During the Clinton Administration, the internet grew from the realm of hobbyists into a mainstream, thriving marketplace of ideas and goods. The internet became a driver of economic growth, and a tool that today helps us all live more efficient lives. Policies that the Clinton Administration pursued were critical to helping that transition occur. We must make sure that the federal government today similarly adopts policies that help blockchain technology move from its main use now—cryptocurrency—to become a driver of wider economic growth and nationwide efficiency.

Blockchain promises potential transformational benefits, but we also need to understand the potential pitfalls that come with the widespread use of blockchain technology. We must also make sure we go beyond the hype and understand the real limitations of the technology. I am glad to have Mr. Aaron Wright, a blockchain expert, and Mr. Chris Jaikaran, from the Congressional Research Service, who can both address potential concerns arising from greater use of blockchain technology.

Again, I am excited that the Committee is covering this important, emerging technology and hope for more hearings on similar topics in the future.

Thank you to all of our witnesses today. I yield back the balance of my time.

[The prepared statement of Mr. Lipinski follows:]

OPENING STATEMENT
Ranking Member Daniel W. Lipinski (D-IL)
of the Subcommittee on Research and Technology

House Committee on Science, Space, and Technology
Subcommittee on Oversight
Subcommittee on Research and Technology
Beyond Bitcoin: Emerging Applications for Blockchain Technology
February 14, 2018

Thank you Chairman Abraham and Chairwoman Comstock for holding this hearing on emerging applications for blockchain technology. And thank you to the expert panel for being here this morning to help us understand the promises and potential limitations of this technology.

As my colleagues have noted, blockchain technologies have the potential, among other benefits, to increase security and reliability of information and decrease fraud and transaction costs across many sectors of our economy. Blockchain technologies also raise important legal and regulatory questions, including how to balance privacy and security while maintaining accountability.

As NIST made clear in its recent Blockchain Technology Overview publication, blockchain remains a nascent and poorly-understood technology. Between the myriad potential applications, the policy considerations, and the possibility of quantum computing rendering the current system of cryptography obsolete, there are many important research questions. These include constructive technologies for blockchain, new cryptographic methods, common standards and protocols, and how blockchain can best be applied across different sectors and for different purposes.

I was surprised that a simple search of active National Science Foundation research awards using the search terms 'blockchain' and 'distributed ledger' yielded only 16 results. No doubt this total far undercounts the number of NSF awards that may have relevance to blockchain technology, and I imagine that other agencies and the private sector are also funding research in this area. But perhaps this also reflects just how nascent a field of research blockchain is. Just in the last year or two, several science and engineering journals have issued calls for submissions for special issues focused on blockchain and distributed ledger technologies.

Today's hearing is a 101 for Committee Members – a chance for us to unpack some of the mystery and mythology around blockchain technology and develop a better understanding of the potential and pitfalls alike. Our panel today represents a diverse set of expertise and viewpoints on blockchain technology that will illuminate some of the sectors where blockchain is having and will have an impact. I look forward to the testimony and discussion.

I yield back.

Chairman ABRAHAM. Thank you, Mrs. Comstock.

I'm going to introduce our witnesses now. Our first witness today is Mr. Chris Jaikaran, an Analyst in Cybersecurity Policy with the Congressional Research Service. Mr. Jaikaran previously worked for the Department of Homeland Security starting in 2005 as a Program Analyst before being promoted in 2008 to Planner. He holds a bachelor of arts degree from Syracuse University, a master's degree in public policy from George Mason University, and a graduate certificate in cybersecurity fundamentals from the Naval Postgraduate School.

Dr. Charles Romine, our second witness, is a Director of Information Technology at NIST. Dr. Romine joined NIST in 2009 as an Associate Director for Program Implementation. In November 2011, Dr. Romine became the Director of Information Technology Laboratory at NIST. Dr. Romine received both his bachelor's of arts degree in mathematics and a Ph.D. in applied mathematics from the University of Virginia.

Mr. Jerry Cuomo, our next witness, is an IBM Fellow and a Vice President of Blockchain Technologies at IBM. Mr. Cuomo has worked with IBM since 1987 as an engineer with IBM Research. He was promoted in 2001 to an IBM Distinguished Engineer, and in 2006 he became an IBM Fellow. He received a master's degree in computer science from New York University Polytechnic School of Engineering.

Mr. Frank Yiannas, our fourth witness, is Vice President of Food Safety at Walmart. Mr. Yiannas previously worked for Walt Disney World as Director of Safety Health from 1989 to 2008. He holds a bachelor's degree of science and microbiology from the University of Central Florida and a master's degree in public health from the University of South Florida.

Our last witness, Mr. Aaron Wright, is an Associate Clinical Professor and Co-Director of the Blockchain Project at the Benjamin N. Cardozo School of Law. Mr. Wright holds a bachelor's of arts degree from Tufts University and a juris doctor from the Benjamin N. Cardozo School of Law.

I now recognize Mr. Jaikaran for five minutes to present his testimony.

TESTIMONY OF MR. CHRIS A. JAIKARAN, ANALYST IN CYBERSECURITY POLICY, GOVERNMENT AND FINANCE DIVISION, CONGRESSIONAL RESEARCH SERVICE

Mr. JAIKARAN. Thank you. Chairs Abraham and Comstock, Ranking Members Beyer and Lipinski, and Members of the Committee, thank you for the opportunity to testify today on blockchain. My name is Chris Jaikaran, and I'm an Analyst in Cybersecurity Policy at the Congressional Research Service. In this role I research and analyze a variety of informational technology issues to include blockchain. My testimony today includes an explanation of blockchain, potential applications for it, limitations and concerns in using it, and potential considerations for Congress.

Blockchain is not a new technology. Rather, it is an innovative way of using technologies we already have. The technology allows parties that may not trust each other to agree on the current dis-

tribution of assets, who has those assets—and who has those assets so they may conduct new business.

But while there has been hype surrounding blockchain, it also has certain pitfalls that may inhibit its utility. Blockchain is a digital ledger that allows parties to transact without the use of a central authority. In this ledger, transactions are grouped together in blocks, which are cryptographically tamperproof, and those blocks are cryptographically chained together in a way that creates an indisputable history. With blockchain, the use of a third-party can be avoided because, as transactions are added, the identities of the parties conducting those transactions are verified and the transactions themselves are verifiable by other users.

The strong relationship between identities, transactions, and the ledger enables parties that may not trust each other to agree on the state of resources as logged in that ledger. With that agreement, they may conduct a new transaction with a common understanding of who has which resource and their ability to trade that resource.

Blockchain is not a new single technology. Rather, it uses existing technologies in a novel way. Blockchain is enabled by asymmetric key encryption, pass values, Merkle trees, and peer-to-peer networks. My written statement goes further into these.

Blockchain is not a panacea technology. A blockchain records events as transactions when they happen, in the order they happen, and in an add-on-only manner. Previous data on the blockchain cannot be altered, and users of the blockchain have access to the data on the blockchain in order to validate the distribution of resources. Some advocate the use of blockchain when a combination of off-the-shelf database, cloud, and identity management technology would likely be more appropriate. An advantage to blockchain emerges when the users want the ledger to be undeniable and traceable.

Though there are benefits to blockchain, there are also pitfalls and unsolved conditions which may inhibit blockchain use. Some of those concerns are data portability, ill-defined requirements, key security, user collusion, and user safety. My written statement elaborates on these further.

As with adopting any technology, users must examine business, legal, and technical aspects of that technology. What is the business case for the technology? Do customers demand attributes which it provides? Or will employees benefit from them? What are the legal implications for using the new technology? Will adhering to compliance regimes be made easier or more difficult through using it? Will data help the new technology be accessible to auditors for review, or will it inhibit regulated transparency? Finally, what are the specific technologies that will be adopted? What are the attributes of that technology and how will it affect current business practices and how will they adapt over time? Blockchain is currently being tested by industry but at this time does not appear to be a complete replacement for existing systems.

My written statement provides a few examples of how blockchain is being employed, piloted, or proposed. One such example is to manage electronic health records. In this example, actual medical records are retained on provider systems, but a record of that

record is published to the blockchain. As identities are cryptographically signed to include those of patients, providers, payers, and other parties, the patient can manage who has access to those records by publishing access rights to specific identities on the blockchain. This is designed to shift the control of these records toward the patient. While technically feasible, this proposal would likely still face federal and state privacy laws, as well as a lack of standards, data processing, and storage, which may inhibit its adoption.

Through the adoption of blockchain—though the adoption of blockchain is in its early stages, Congress may have a role to play in several areas, including providing oversight of federal agencies seeking to use blockchain for government business or regulating industries using blockchain. Some federal agencies are seeking to better manage identities, assets, data, and contracts through the adoption of blockchain technology. In addition, some of—federal agencies are issuing guidance on industry use of blockchain and whether or not the current legal framework governs blockchain use.

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

[The prepared statement of Mr. Jaikaran follows:]

Congressional Research Service
Informing the legislative debate since 1914

TESTIMONY

Statement of

Chris Jaikaran
Analyst in Cybersecurity Policy

Before

Committee on Science, Space and Technology
Subcommittee on Oversight & Subcommittee on Research and Technology
U.S. House of Representatives

Hearing on

"Beyond Bitcoin: Emerging Applications for Blockchain Technology"

February 14, 2018

Congressional Research Service
7-5700
www.crs.gov

CRS TESTIMONY
Prepared for Congress

Introduction

Chairs Abraham and Comstock, Ranking Members Beyer and Lipinski, and Members of the Committee, thank you for the opportunity to testify on blockchain today. My name is Chris Jaikaran and I am an Analyst in Cybersecurity Policy at the Congressional Research Service. In this role, I research and analyze a variety of information technology issues of interest to Congress, including emerging technologies like blockchain.

My testimony today includes an explanation of blockchain technology, potential applications for it, limitations and concerns in using the technology, and potential considerations for Congress. My testimony today is based solely on publicly available information and CRS analysis.

Blockchain is not a new technology, rather it is an innovative way of using technologies we already have. This is done so that parties who may not trust each other can agree on the current distribution of assets and who has those assets, so that they may conduct new business. But, despite the hype surrounding the technology, it has certain pitfalls which can inhibit its utility.

Blockchain Explained

A blockchain is a digital ledger that allows parties to transact without the use of a central authority to validate those transactions. The use of a central authority (i.e., a third party) can be avoided because in a blockchain, as transactions are added, the identities of the parties conducting those transactions are verified, and transactions are verified as they are added to the ledger as a block of transactions. The ledger is auditable because each block of transactions is dependent upon the previous block in such a way that any change would alert other users of a change to the history of transactions. The strong relationships between identities, transactions, and the ledger enable parties that may not trust each other to agree on the state of resources as logged in the ledger. With an agreement on that history, parties may then conduct a new transaction with a shared understanding of who has which resource and of their ability to trade that resource.

Technology

Blockchain is not a new technology; rather it is an innovative way of using existing technologies. Four particular technologies are used to enable blockchain technologies: asymmetric key encryption; hashes; Merkle trees; and peer-to-peer networks.

Asymmetric Key Encryption

Asymmetric key encryption, also known as a public-private key cryptosystem, functions to create identities on a blockchain. A user creates two elements, a public key which helps identify their transactions on the blockchain, and a private key which is necessary to conduct a transaction with the public key. Asymmetric encryption allows for the authentication of users because only those with the private key can decrypt data encrypted with the public key or encrypt the data for public key decryption, thereby creating a signature.[1]

The public key may be broadcast on the blockchain itself, or may be tied to an address which is broadcast instead. In some blockchain systems, the real-world identity of each address or public key is logged so that individual users may be tracked. In others, a user may be able to generate public and private keys

[1] For more information on encryption see CRS Report R44642, *Encryption: Frequently Asked Questions*, by Chris Jaikaran.

independently and broadcast the public key or address without identifying themselves, creating a pseudonymous identity on the blockchain.

In a blockchain, the public key is used to identify a user on the blockchain and verify the resources tied to that user's public key or address. The resource could not be used unless the holder of the public key to which the resource is tied unlocks (or decrypts) the resource with their private key, allowing it to be transferred to another identity on the blockchain (a public key or address) and locked with that second user's private key. This transaction would be logged on the blockchain, so that other users could verify the resource has changed possession.

An example of asymmetric key encryption, other than blockchain, is used daily when a user connects to a website via Hypertext Transfer Protocol-Secure (HTTPS). To enable the secure connection to the website, a user starts the process by sending a request to the site. The site would then send their public key to the user, and the user's computer would then generate a new key (to be used in the HTTPS connection), encrypt it with the website's public key and send that back. The user knows that only the website that has the private key could decrypt the information the user just sent. With the new, user-generated key, the website would create the secure connection with the user, indicated to the user by the HTTPS icon (frequently a lock symbol) in the browser window.

Hash Values

A hash uses similar mathematical functions as an encryption method to produce a string of characters as an output given some data as input. This is a one-way function, meaning a hash value may be created from an input, but the input cannot be recreated from the hash. In blockchains, a number of transactions are tranched together to make a single block, which is then hashed.

Hash values are used to validate the integrity of a block. Any alterations to the transactions that make up a block will change the hash value of the block as a whole. If a block's hash value stays the same over time, users can be sure that the transactions in that block have not been tampered with. This allows users on the blockchain to determine whether or not they can trust the history on the blockchain.

Merkle Trees

Databases and ledgers are large and are constantly being edited as new entries are added and data is modified or deleted. If one wanted to have a hash value for the database, one would have to constantly hash it, and maintain a way of ensuring they have the right hash value to align with the current state of the system in order to judge its integrity. Additionally, the larger the database becomes, the more computationally intensive hashing it becomes. A Merkle tree is a cryptographic concept introduced by Ralph Merkle in 1980 as a way around this problem.[2]

In a Merkle tree, data is segmented apart from a single whole data file. There is a root block of data with a hash value, then subsequent blocks of data (sometimes referred to as child, branch, or leaf blocks) that have their own hash value. Each subsequent block of data takes the hash value of their previous block (sometimes referred to as a parent block) as an input in the creation of the hash value of the new block. This creates a chain or tree of hash values, cryptographically tying new blocks of data to previous ones in a way that prohibits altering previous data. If data in a previous block were to be added, modified, or deleted, the hash value of the subsequent blocks of data would not compute to what they would need to be, alerting users that a change was made. This also allows hash values to be created for smaller, more

[2] Ralph C. Merkle, "Protocols for Public Key Cryptosystems," conference paper, Oakland, CA, April 1980, at www.merkle.com/papers/Protocols.pdf.

discrete blocks of data which is computationally less resource intensive than rehashing an entire set of data each time an edit is made.

Blockchains borrow the concept of Merkle trees to make hash chains. In a blockchain, a first block is created and a hash value is computed for it. This is the root block. Subsequent blocks then use the hash value of the previous block in the chain as one of the inputs to create that next block. This chaining of hash values creates a strong relationship between blocks on the chain, and an auditable and immutable record of the transactions on the blockchain.

Peer-to-Peer Networks

A peer-to-peer (P2P) network allows a disparate system of computers to connect directly with each other without the reference, instruction, or routing of a central authority. P2P networks allow for the sharing of files, computational resources, and network bandwidth among those in the network.

In a blockchain, a P2P network allows the users of the blockchain to broadcast directly to and among each other the current state of the blockchain (so that users may agree on the history of transactions), and when a new block is added. This also allows for redundancy of the data in the blockchain, as any user may download a complete copy of the current ledger of transactions and add a new block, so that there will not be a single point of failure for the blockchain if a node on the network goes down.

In some blockchain implementations, users do not host copies of the ledger among themselves. Instead, users use a cloud service provider (CSP) to maintain active and back-up copies of the blockchain, and compute the transactions and blocks as they happen. In these cases, peer-to-peer networking is necessary to run the blockchain. While the CSP is not a central validating authority in this example, it does become a third party to the transaction.

Transactions in a Blockchain

Blockchains consist of a series of blocks of transactions. A transaction is an event in which a resource or asset changes possession from one party to another. These individual transactions are signed by the users engaging in those transactions through the use of public-private key encryption. Because the private key is necessary to release and accept a resource in a transaction on the blockchain, the users transacting on the blockchain are, in effect, signing the transaction to ensure its security. Transactions are grouped together and made into a block which is validated upon its creation through the act of *mining* for the creation of blocks (mining is further explained below). The integrity of the entire ledger is ensured by each block having a hash value which is dependent on the previous block's own hash value. Each of these three steps relies on strong cryptography which ensures the validity of the ledger.

Transactions may not post immediately to a blockchain. If a lot of transactions are occurring in a short amount of time, the blockchain platform may create a pool of pending transactions which are processed in accordance with rules of that blockchain – which may allow for fees, user priority, or some other method to post certain transactions into a block before others.

Blockchain Governance

A blockchain can be public or private. In a *public* blockchain, anyone can create a public-private key pair and download a copy of the blockchain. This is usually accomplished through a software package which governs transactions on the blockchain. In a *private* blockchain, the membership of users on the blockchain is controlled. In private blockchains, the users authorized to participate may be bound by contractual relationships with each other, their blockchain addresses may be closely tied to their real-world identities, or participation on that blockchain may be agreed upon by other members in the

blockchain. In any case, members of a private blockchain may be more trusting of each other than in a public blockchain.

A blockchain can be permissioned or permissionless, which is independent of whether the blockchain is public or private. A *permissioned* blockchain is one in which the permission of a user is assigned to them. Some users may only be able to view a whole or portion of the blockchain, others may be able to add new blocks. In this system, the administrator(s) do not serve as a central authority, since they do not govern the creation of blocks on the blockchain, just the rights of users on the blockchain. In a *permissionless* blockchain, all users have equal rights, with any one able to download the full blockchain and have an opportunity to potentially add additional blocks.

Discussing a blockchain as public or private refers to the level of freedom users have to creating identities on that blockchain. Discussing a blockchain as permissioned or permissionless refers to the level of access the user would have on that blockchain. Users on the blockchain must reach *consensus* on the rules for creating and publishing new blocks and resolving disagreements.

Blockchains have users and nodes on the blockchain platform. The *users* on a blockchain could be the individuals, businesses, or other identities which have a public-private key pair and conduct transactions. A *node* is a computing system on that blockchain. A user may have a node (e.g., an individual's computer or a business's computing network), or a group of users could pool resources to create a single node (e.g., users who share their computing power to mine for new blocks on the blockchain). In a blockchain platform that uses a CSP, the CSP is a node on the blockchain, but may also be a user.

The creation and publication of a new block in the blockchain is called *mining*. In mining blocks, users seek to add the next block to the chain. Mining is incentivized by improving the user's standing in that blockchain, either through a monetary, reputational, or stake award for adding new blocks. New blocks may be added to a blockchain through a variety of methods. Three such methods are proof of work, proof of stake, and round robin.

In a *proof of work* scheme, those seeking to add a block to the blockchain are presented a difficult computational problem. By solving the problem, they win the opportunity to post the next block and possibly a reward for doing so. Their solution is broadcast to others users who can validate it immediately without going through the same resource intensive computation required to solve the problem. In this scheme, the problem is frequently a direction that the hash value contains certain elements (e.g., the value begins with four zeros). In order to produce a hash value with those elements, additional information is added as an input (along with the previous block's hash value, the transactions in the block, data and time information, etc.). This additional information is called a nonce, and could be as simple as a number which would alter the hash value. Finding the nonce value that solves the problem wins for that miner the right to publish the next block.

In a *proof of stake* scheme, the next block may be awarded to the user who has an appropriate stake in that block. This may be because the block contains transactions regarding that user. Or, the user has an X percentage of stake in that blockchain, so they are awarded the right to publish X percent of blocks to that blockchain. Proof of stake schemes are computationally less resource intensive than proof of work. In the *round robin* scheme, users on the network take turns adding new blocks. Because some level of trust is necessary for round robin schemes to work, they are used in permissioned blockchains.

If there is a disagreement in the blockchain, most users on the node will use the longest chain on the block as the valid ledger and use that one as the basis for future transactions. In the event that two different miners publish blocks at the same time, and those blocks contain different information, blockchains may allow both blocks to be published for that round, then allow the system to resolve itself upon the publication of the next block, which would then create the largest chain of transactions, and therefore, the most trusted ledger. Another way of resolving disagreements is through using byzantine fault tolerance,

whereby users on the blockchain platform will vote on which block they choose to accept and the plurality of votes determines the next block to be published.[3]

Blockchain Uses

Blockchain is not a panacea technology. A blockchain records events as transactions when they happen, in the order they happen, in an add-on only manner. Previous data on the blockchain cannot be altered, and users of the blockchain have access to the data on the blockchain in order to validate the distribution of resources. If an entity has critical data that it wants to share, a combination of current database, cloud, and identity management technologies will likely be adequate for its needs. However, if the entity seeks to have its data be immutable and auditable, then a blockchain may be appropriate. While an entity may find immutable and auditable transactions enticing, the inability to edit those transactions (even in cases of error, when an additional invalidating transaction will be necessary) may still make blockchain a suboptimal record keeping technology. Examples of blockchain uses that are in use, are being piloted, or have been discussed are listed below, in alphabetical order.

Cryptocurrencies

Bitcoin is the most popular cryptocurrency, garnering the largest market share, and arguably initiated the interest in blockchain technology. Cryptocurrencies, like Bitcoin, are built to allow the exchange of some digital asset of value (the cryptocurrency) for a good or service.[4] They are frequently permissionless and use a proof of work model to add blocks. In these systems, anyone can create a *wallet* which includes their private key, their public key, and an address which is derived from their public key. They then acquire (through mining, or purchase) the cryptocurrency, and add that as a transaction to the blockchain, so that their address is linked to their value. If they purchase something, they will then unlock the cryptocurrency with their private key, transfer it to the seller who then locks it with their private key. This transaction is published to the blockchain so all users are able to validate that the buying user has that much less of the cryptocurrency and the selling user has that much more of it. Each cryptocurrency has its own blockchain.

Healthcare

There have been a variety of proposals for using blockchain in the healthcare sector, many of which involve the management of electronic health records (EHRs). One such proposal is to use the blockchain to authenticate patients and health providers on a blockchain in order to enable the sharing of EHRs.[5] In this proposal, the EHR is held on a system hosted by the provider, but existence of the record is published to the blockchain, and the patient may use the blockchain to authorize who may have access to that record. However, applications of blockchain for healthcare implicate both federal laws (i.e., the Health Insurance Portability and Accountability Act of 1996, HIPPA, P.L. 104-191, and the Health Information Technology for Economic and Clinical Health Act, HITECH, Title XIII of Division A of P.L. 111-5) and state health record privacy laws, which may inhibit its use.

[3] Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3 (July 1982).

[4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," paper, October 2008, at https://bitcoin.org/bitcoin.pdf.

[5] Ariel Ekblaw, Asaph Azaria, John Halamka, and Andrew Lippman, "A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data," paper, August 2016, at https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf.

Identity Management

Identity management use of blockchain draws upon asymmetric encryption and immutable transactions as strengths. In this use, a user has a private key to validate transactions made with their public key, which are then published (or data about the transaction are published) to the blockchain. This ensures that only the user with the private key is able to conduct transactions and resolves the double-spend problem because the transaction is published so other users can validate the distribution of resources to that public key or address.[6] However, this form of identity management requires both a computing device and an Internet connection to work. Private entities may be able to require users to maintain a compatible device for their blockchains, and the Internet connection required to execute a transaction on the blockchain, but other entities (like the public sector) may face difficulty in moving to a blockchain-only identity management model because some of their customer base lack the computing elements necessary to conduct the transaction—creating a cost-sharing problem.

Provenance

Because asymmetric encryption allows for the authentication of users, blockchain has been suggested as a solution to the provenance of items. Provenance refers to the ability to know the history of an item, so that users can be assured that they may be legitimate consumers of the item. By using blockchain, proponents seek to enable the transfer of property, rights, or goods without the clearance of a third-party intermediary, thereby reducing costs. In this model, a user would publish to the blockchain that they have the right to an asset—the user's claim to that right would still need to be verified, which may be governed by the rules of the blockchain—and others may purchase or license that asset, which would then be published to the blockchain for other users to verify.

There are examples of using blockchain for both physical and digital item provenance. Cook County, Illinois has investigated using blockchain to track the transfer of land.[7] In its pilot, it sought to track the conveyance of real property on a blockchain. This could have the potential to affect the titling industry as anyone could verify that a seller is legally in possession of the property they seek to sell and are in a position to conduct a valid sale. For digital items, Kodak has announced that it will endorse blockchain technology to track the rights of digital images and provide a way for content users to pay for the license to use an image. However, implementation concerns have generated significant criticism among industry analysts on Kodak's plans.[8]

Smart Contracts

The digital nature of blockchain has led to it being associated with smart contracts. A contract in the physical world is an agreement among parties that upon execution of certain conditions, a transfer of assets will occur. A smart contact codifies these attributes in code, so that machines can validate that conditions are met, and initiate the transfer of assets. In addition to the parties engaging in the transaction, other users of the blockchain platform may provide computational resources necessary to process or

---

[6] The double spend problem refers to transactions which may not immediately post, allowing a party to spend that resource many times before it is reflected in ledgers. For more information see David Mills et al., "Distributed Ledger Technology in Payments, Clearing, and Settlement," *The Federal Reserve Board* paper, 2016, at https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf.

[7] John Mirkovic, "Blockchain Pilot Program Final Report," report, May 30, 2017, at http://cookrecorder.com/wp-content/uploads/2016/11/Final-Report-CCRD-Blockchain-Pilot-Program-for-web.pdf.

[8] Kevin Roose, "Kodak's Dubious Cryptocurrency Gamble," *The New York Times*, January 30, 2018, at https://www.nytimes.com/2018/01/30/technology/kodak-blockchain-bitcoin.html.

validate the contractual transaction, thereby gaining a stake in the transaction or contributing to the verification of the transaction on the ledger.

An example of a smart contract platform is Ethereum, which allows users to build smart contracts on a blockchain platform. In Ethereum, users build their smart contract and pay fees so that other users contribute computational resources to enable the smart contracts and validate the transactions.

Supply Chain Management

Supply chain management of physical and digital goods on blockchain is similar to the smart contract application. In this application, goods are tagged with a digital value (e.g., a scannable code for physical goods, or a tracker for digital goods) and as it passes from one entity to the next, that entity accepts it and then transfers it to another using its public-private key. These transactions are added to the blockchain so various participants are able to track the disposition of the good from creation through distribution, to retail, and potentially to the end user.[9] However, this system will only allow for accountability of which party had control of the real-world item at which point. As the item itself does not contain traceable code, it must be affixed with a tracker, such as a scannable code or a sensor which enables its tracking. Someone in this chain may still manipulate the item, alter trackers, or otherwise adulterate items in the supply chain which may not be logged on the blockchain. An example of supply chain management on a blockchain platform is tracking of minerals from the Democratic Republic of the Congo that will be used to build batteries.[10]

Blockchain Concerns

The cryptographic attributes of blockchain present a compelling reason for its use over other technologies. But there are persistent pitfalls and unsolved conditions which may inhibit wide use of blockchain. Some of those concerns are discussed below.

Data Portability

As with other record keeping systems, once data is logged in one system, transferring that data to a new system may be problematic. This problem persists in many blockchain applications. Once a user chooses to use one blockchain, they are unable to remove their previous records of transactions and transfer them to a new system as those transactions are part of the blockchain and any alteration to the chain would result in users being unable to generate legitimate hash values for new blocks. The existence of that data is permanent on the blockchain. Additionally, if a user seeks to copy their data from one blockchain to another, there are no standards for data construction from one blockchain to the next, so all the elements of data from one blockchain may not be imbedded in another, nor will how they process public-private keys or hash values. The lack of standards in blockchain technologies extends beyond how data is stored to how public-private keys are generated, how hash values are generated, and how data is broadcast across peers. The lack of standards effectively means that once a user chooses one blockchain for their use, they may be unable to transfer to another blockchain. While they may be able to recreate their current allotment of resources on a new chain and conduct transactions from that point, their history will be encapsulated on the previous chain.

---

[9] For more information in supply chain issues and blockchain, see CRS In Focus IF10810, *Blockchain and International Trade*, by Rachel F. Fefer.

[10] Barbara Lewis, "Blockchain to Track Congo's Cobalt from Mine to Mobile," *Reuters*, February 2, 2018, at https://www.reuters.com/article/us-mining-blockchain-cobalt/blockchain-to-track-congos-cobalt-from-mine-to-mobile-idUSKBN1FM0Y2.

Ill-Defined Requirements

As with adopting any technology, adopters must examine the business, legal, and technical aspects of adopting blockchain.[11] Because blockchain is in the early stages of its development and adoption, users are likely to face a set of questions that do not have clear answers. What is the *business* case for the technology? Do customers demand attributes that the new technology provides? Will employees benefit from them? What are the *legal* implications for using the new technology? Will adhering to compliance regimes be easier or more difficult? Will data held in the new technology be accessible to auditors for review? Will it inhibit regulated transparency? Finally, what particular *technology* will be adopted? What are the attributes to that technology (e.g., using one hashing algorithm instead of another)? How will it affect current practices, and how might it adapt over time?

Key Security

As with other forms of encryption, the creation, storage, and loss of control of the private key creates problems that are unsolved. If a user were to have their device that stores their private key compromised, an attacker would have access to their private key and be able to transfer resources from their public key to another public key or address controlled by the attacker. If the user's hard drive fails, or they forget or otherwise lose their private key, they effectively lock the resource tied to their public key forever, inhibiting any other transaction with that asset.

User Collusion and Control

Groups of users on the blockchain may combine computing resources and collude to mine blocks. In some blockchain implementations this is allowed and encouraged. However, it does present a situation where groups of users may wield unintended influence over which transactions make it into a block, and the blocks that are posted. Additionally, a user, or group of users (the attacker) with sufficient computational power may be able to recreate the blockchain, thereby altering previous transactions and broadcasting to blockchain users that the attacker's chain is valid. As it would be the longest chain, others may automatically accept it, even though it was in error. This is called the 51% attack. While it is computationally difficult to carry out against established blockchains, it may allow an opportunity for nefarious users to corrupt a new, or up-start blockchain platform, which have shorter ledgers, thereby ensconcing them as controllers of block creation.

User Savviness and Safety

Another issue that affects other technologies, and one that applies to blockchain, is the level of comfort and knowledge a user must have with the technology in order to properly and safely use it. For instance, many drivers do not know how a car works but can still safely drive a car. Or, many users do not know how computers and networking work, but can still type out and send an email. Lay-user participation is possible because certain design decisions were made by government (e.g., seatbelt requirements and the need for a driver's license) and engineers (e.g., simple user interfaces) that enable users to use those technologies. As blockchain technology is developed, adopted, and used, similar design requirements may be necessary to ensure proper use and safe adoption of the technology. In addition to the use of blockchain technology itself, users may also need to be aware of its pitfalls and tradeoffs before adopting it. For instance, stories have circulated that users who own Bitcoin have lost access to their private keys, thereby prohibiting the use of that asset in the future – they effectively lost the asset, and without a central authority, have no recourse to restore that asset.

[11] Manu Sporny, "DHS Blockchain/Distributed Ledger Conference," October 10, 2017.

Potential Considerations for Congress

Although blockchain is already being used as a financial instrument, it is relatively nascent in other sectors of the economy. Because of its novelty, blockchain is being piloted by industry, but at this time does not appear to be a replacement for existing systems. Given these conditions, the technology does not contain the same level of adoption that previous technology had when facing potential legislative action. However, Congress can still provide oversight of federal agencies seeking to (1) use it for government business, and (2) regulate industries using blockchain.

The General Services Administration and the Department of Homeland Security are examining blockchain as a way to achieve efficiencies in the current business of government.[12] In these examinations, the federal government is seeking ways to better manage identities, assets, data, and contracts.

Agencies such as the Securities and Exchange Commission and the Commodities Futures Trading Commission are issuing advisories to industry concerning blockchain technology. In some cases, these actions are to positively declare that the current legal framework governing other transactions also apply to transactions on a blockchain.[13]

In both of these areas, Congress may want to evaluate whether agencies are achieving Congress's policy goals. These goals may be technology agnostic and thus already established, or Congress may develop new policy goals for the adoption of emerging technology across a variety of sectors.

Conclusion

Thank you again for the opportunity to testify today. I look forward to your questions. If you require further research or analysis on this topic, or other policy issues before Congress, my colleagues and I at CRS are ready to assist you.

12 For examples, see https://emerging.digital.gov/blockchain-forum/, https://emerging.digital.gov/blockchain-programs/, and https://www.dhs.gov/science-and-technology/news/2017/09/25/news-release-dhs-st-awards-750k-virginia-tech-company.

[13] SEC, "Investor Bulletin: Initial Coin Offerings," alert and bulletin, July 25, 2017, at https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.

Biography

Chris Anwar Jaikaran
Congressional Research Service

Mr. Jaikaran is an Analyst in Cybersecurity Policy in the Government and Finance Division of the Congressional Research Service. He specializes in cybersecurity issues, particularly those with an intersection to homeland security. He holds a BA from Syracuse University, an MPP from George Mason University and a post-graduate certificate from the Naval Postgraduate School.

Pronunciation: Jai-kuh-ran

Chairman ABRAHAM. Thank you, Doctor.

I now recognize Dr. Romine for five minutes to present his testimony.

TESTIMONY OF DR. CHARLES H. ROMINE, DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Dr. ROMINE. Chairman Abraham, Ranking Member Beyer, Chairwoman Comstock, and Ranking Member Lipinski, and Members of the Subcommittees, I'm Chuck Romine, the Director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology, also known as NIST. Thank you for the opportunity to appear before you today to discuss NIST's role in blockchain technologies.

Blockchains are defined as immutable digital ledger systems implemented in a distributed fashion that is without a central repository. At their most basic level, they enable a community of users to record transactions in a ledger that is public to that community so that transactions cannot be changed once published without the community knowing.

The core ideas behind blockchain technology emerged in 1991, and this technology became widely known in 2008 when the blockchain idea was combined with several other technologies and computing concepts to enable the creation of modern cryptocurrencies. Cryptocurrencies such as Bitcoin are electronic money protected through cryptographic mechanisms or blockchains for secure funds transfer. Blockchains are often viewed as synonymous with Bitcoin, but its applications are broader than fund transfer security. Its use cases vary from banking to secure supply chains to insurance and, as you've heard, health care.

The use of blockchain technology, however, is not a silver bullet. Some issues must be considered such as how to deal with malicious users, how controls are applied, and the limitations of any blockchain implementation. NIST has a strong research program in advancing key components of the blockchain such as measurement science for computer security, cryptography, and cryptographic key management, creating solutions to real-world problems.

In January 2018 NIST published a draft report "Blockchain Technology Overview," which is now out for public comment. The report introduces the concept of blockchain, discusses its use in electronic currency, and shows its broader applications.

NIST has conducted extensive research on asymmetric key cryptography, also referred to as public-private key cryptography, which is a fundamental technology to secure blockchain technologies. NIST develops, maintains, and tests implementations that meet NIST's standards and guidelines for key generation and derivation, key establishment, and key exchanges.

Because blockchains are not centralized, users must manage their own private keys, meaning if one is lost, anything related to that private key, such as digital assets, is lost. If a private key is stolen, the attacker will have full access to all assets controlled by that private key. Therefore, security of private keys is critical. When the news media reports that Bitcoin was stolen from, it almost certainly means that the private keys were found and used

to sign a transaction sending the money to a new account, not that the system itself was compromised.

Looking forward, quantum computers will be a threat to blockchain technologies because they will be able to break the code and crack the public key cryptosystems. NIST is leading the global effort to ensure new encryption is available to industry and built into products before quantum computers emerge.

Research at NIST to more generally use blockchain platforms is ongoing via the NIST blockchain workbench, which provides flexible testbeds that NIST researchers can use to implement theoretical solutions. This hands-on experience is essential to complement NIST interactions with industry and documentary standards research when NIST issues papers, guidance, tools, and references.

Blockchains are a new and exciting technology that have the potential to address real corporate and consumer needs, but much work still needs to be done to understand this technology, to bring out its potential, and let markets reward usable and secure implementations that meet real customer needs.

NIST will continue its research and development in the foundational cryptography that blockchains use. We will continue to learn from our research and continue to build collaborations with industry in the publication of guidelines. NIST also continues to work with international standards bodies that have started study groups and technical committees to initiate standards work for blockchains. This is an exciting time for blockchain technology as it emerges into markets and sectors.

Thank you for the opportunity to testify on NIST's work regarding blockchain, and I'll be happy to answer any questions that you may have.

[The prepared statement of Dr. Romine follows:]

Testimony of

Charles H. Romine, Ph.D.
Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the

United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight
and
Subcommittee on Research and Technology

"Beyond Bitcoin: Emerging Applications for Blockchain Technology"

February 14, 2018

Introduction

Chairman Abraham, Ranking Member Beyer, Chairwoman Comstock, Ranking Member Lipinski and members of the Subcommittee, I am Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in cybersecurity and blockchain.

The Role of NIST in Cybersecurity

With programs focused on national priorities, from advanced manufacturing and the digital economy to precision metrology, quantum science, and biosciences, NIST's overall mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, starting with the development of the Data Encryption Standard, when the potential commercial benefit of this technology became clear. NIST's role, to research, develop, and deploy information security standards and technology to protect the Federal Government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA 2002) (Public Law 107-347[1]), and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST standards and guidelines are developed in an open, transparent, and collaborative manner that enlists broad expertise from around the world. While developed for federal agency use, these resources are often voluntarily adopted by other organizations, including small and medium-sized businesses, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective and accepted globally. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

Blockchain

Blockchains are immutable digital ledger systems implemented in a distributed fashion—that is, without a central repository—and usually without a central authority. At their most basic level, they enable a community of users to record transactions in a ledger that is public to that

[1] FISMA 2002 was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347; 116 Stat. 2899).

community, so that transactions cannot be changed, once published, without the community knowing.

These transactions are secured with cryptographic hashes, and transactions are signed and verified using public/private key pairs. The transaction history is summarized to efficiently and securely record a chain of events so that any attempt to edit or change a past transaction requires all subsequent blocks of transactions to be recalculated.

In 2008, the blockchain idea was combined in an innovative way with several other technologies and computing concepts to enable the creation of modern cryptocurrencies, which are electronic money protected through cryptographic mechanisms instead of a central repository. The first such blockchain-based approach was Bitcoin, followed by Ethereum, Ripple, and Litecoin. As a result, blockchains are often viewed as synonymous with Bitcoin or possibly e-currency solutions in general, but its applications are broader than fund transfer security.

Currency blockchain systems are novel because they store value, not just information. The value is attached to a digital wallet—an electronic device or software that allows an individual to make electronic transactions. The wallets are used to sign transactions sent from one wallet to another, to record the transferred value publicly, and to allow all participants in the network to independently verify the validity of the transactions. Each participant can keep a full record of all transactions, making the network resilient to attempts to alter that record or forge transactions later.

Many electronic cash schemes existed prior to Bitcoin, but none of them were widely used. By adopting blockchain technology, Bitcoin achieved compelling capabilities that promoted its use. The use of a blockchain enabled Bitcoin to be implemented in a distributed fashion so that no single user controlled the currency and no single point of failure existed. Bitcoin's primary benefit is to enable direct electronic financial transactions between users without the need for a third party.

By using a distributed blockchain and consensus-based maintenance, a self-policing mechanism was created, ensuring that only valid transactions are added to the blockchain. Blockchain enables users to be pseudonymous, meaning that the identity of the users is anonymous but their accounts are not—all their transactions could be seen publicly. Also, the distributed maintenance of the blockchain created a completely transparent system, which promoted trust in its use. Blockchain use cases vary from banking to supply chain to insurance and healthcare.

The use of blockchain technology, however, is not a silver bullet. Some issues must be considered, such as how to deal with malicious users, how controls are applied, and the limitations of any blockchain implementation. Once a blockchain is implemented and widely adopted, it becomes very difficult to change it. Once something is recorded in a blockchain, it is usually there forever, and it takes a significant effort—involving a majority of the community—to make a change, even when there is a mistake.

NIST Activities Related to Blockchain

Blockchains use well-known computer science mechanisms (such as linked lists and distributed networking) and cryptographic primitives (such as hashing, digital signatures, and public/private keys) mixed with financial concepts (such as ledgers). NIST has a strong research program in advancing measurement science for computer security, cryptography, and cryptographic key management.

In January 2018, NIST published draft NIST Internal Report 8202 "Blockchain Technology Overview.[2]" The report describes how a blockchain system works and provides a common language for communication among technology developers and users. Organizations considering implementing blockchain technology need to understand important aspects of the technology, and users of this technology need to understand its advantages and disadvantages.

NIST collaborates with experts from industry, academia, and government to strengthen its research portfolio and to create and promote solutions to real-world problems. In September 2017, NIST and the Office of the National Coordinator for Health Information Technology cohosted an industry-wide workshop titled "Use of Blockchain for Healthcare and Research."

On September 18 and 19, 2018, NIST will host the Institute of Electrical and Electronics Engineers (IEEE) Blockchain Summit at its campus in Gaithersburg, Maryland. Researchers and developers from industry and academia will share insights on the status of current usage studies, where new opportunities are surfacing, and critical questions and challenges that need to be addressed to advance blockchain technology.

Cryptography

NIST has conducted extensive research activities on asymmetric-key cryptography, also referred to as public/private key cryptography, a fundamental technology utilized by blockchain technologies. Asymmetric-key cryptography uses a pair of keys—a public key and a private key – that are mathematically related to each other. For Federal information systems, Federal Information Processing Standard (FIPS) Publication 186-4, Digital Signature Standard,[3][4] specifies the Elliptic Curve Digital Signature Algorithm, which is a common algorithm for digital signing used in blockchain technologies.

A private key is usually generated using a secure random function, meaning that reconstructing it is difficult, if not impossible. NIST develops, maintains, and tests implementations that meet NIST's standards and guidelines for key generation and derivation, key establishment, and key exchanges.

---

[2] https://csrc.nist.gov/publications/detail/nistir/8202/draft

[3] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 186-4, Digital Signature Standard, July

[4] . https://doi.org/10.6028/NIST.FIPS.186-4

Because blockchains are not centralized, there is no intrinsic central place for user key management. Users must manage their own private keys, and if one is lost, anything related to that private key—such as digital assets—is also lost. There is no "forgot my password" or "recover my account" feature for blockchain systems. If a private key is stolen, the attacker will have full access to all assets controlled by that private key. The security of private keys is so important that many users rely on secure hardware to store them. When the news media announce that "Bitcoin has been reported stolen," it almost certainly means that the owner's private keys were found and used without permission to sign a transaction sending the money to a new account, not that the system was compromised.

Quantum Computing

The public key cryptographic algorithms used within most blockchain technologies for public/private key pairs will need to be replaced when powerful quantum computers become a reality. It is generally accepted that algorithms that rely on the computational complexity of integer factorization—or work on solving discrete logarithms—will be susceptible to quantum computing. NIST Internal Report 8105, titled "Report on Post-Quantum Cryptography,[5]" describes the impact of quantum computing on common cryptographic algorithms. NIST is currently working on developing, identifying, and selecting the next set of public key cryptography that will be effective when quantum computers come into use. NIST is leading this global effort, which aims to ensure this encryption is available to industry and built into products before quantum computers emerge.

Hash Functions

An important component of blockchain technology is the use of cryptographic hash functions. Blockchain technologies take a list of transactions and create a hash "fingerprint" for the list. Anyone with the same list of transactions can generate the exact same fingerprint. If a single value in a transaction within the list changes, the digest for that block changes, making it easy to discover even minor one-bit changes. Common hashing algorithms used by Bitcoin, Ethereum, and Litecoin are described in FIPS 180-4[6] and FIPS 202[7]. Also, the NIST Secure Hashing website[7] contains FIPS specifications for Federal information systems for all NIST-approved hashing algorithms.

NIST Blockchain Workbench

Research in how to more generally use blockchain platforms is hampered by high entry barriers, mainly resulting from the lack of training material, tools, and testbeds. NIST has developed a

---

[5] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[6] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 180-4, Secure Hash Standard (SHS), August 2015. https://doi.org/10.6028/NIST.FIPS.180-4

[7] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication SHA-3 Standard: Permutation-Based Hash and ExtendableOutput Functions, May 2014. https://csrc.nist.gov/csrc/media/publications/fips/202/final/documents/fips_202_draft.pdf [7] National Institute of Standards and Technology (NIST), Secure Hashing website, https://csrc.nist.gov/projects/hash-functions

blockchain workbench capability, which provides flexible testbeds and workbenches that NIST researchers can use to implement theoretical solutions. This capability also enables researchers to evaluate the potential usefulness of blockchain architectures for various applications. This distributed system is implemented on several servers, provides a graphical user interface, and is supporting a wide range of experimental scenarios developed by NIST. This hands-on experience is essential to complement NIST interactions with industry, as well as NIST research leading to reports, guidance, tools, and references.

NIST Participation in Blockchain Standardization

Under the provisions of the National Technology Transfer and Advancement Act (PL 104-113) and Office of Management and Budget (OMB) Circular A-119[8], NIST is tasked with the role of encouraging and coordinating federal agency use of voluntary consensus standards in lieu of government unique standards, and federal agency participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies to coordinate standards issues and priorities with the private sector through consensus standards developing organizations (SDOs), such as the InterNational Committee for Information Technology Standards (INCITS), Joint Technical Committee 1 of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), the Organization for the Advancement of Structured Information Standards (OASIS), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and other standards organizations such as the International Civil Aviation Organization (ICAO) and the International Telecommunication Union's Standardization Sector (ITU-T). NIST leads national and international consensus standards activities in biometrics, cryptography, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing—all of which are essential to accelerate the development and deployment of information and communication systems that are interoperable, reliable, secure, and usable.

Voluntary Consensus Standards

Most SDOs are industry-led private sector organizations. Many voluntary consensus standards from those SDOs are appropriate or adaptable for the U.S. Government's purposes. OMB Circular A-119 directs the use of such standards by U.S. Government Agencies, whenever practicable and appropriate, to achieve the following goals:

- eliminating the cost to the Federal Government of developing its own standards and decreasing the cost of goods procured and the burden of complying with agency regulation;
- providing incentives and opportunities to establish standards that serve national needs, encouraging long-term growth for U.S. enterprises and promoting efficiency, economic competition, and trade; and
- furthering the reliance upon private sector expertise to supply the Federal Government with cost-efficient goods and services.

[8] "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities," https://www.gpo.gov/fdsys/pkg/FR-2016-01-27/pdf/201601606.pdf

When properly conducted, standards development can result in increased productivity and efficiency in government and industry, greater innovation and competition, more opportunities for international trade, conservation of resources, increased benefits and choices for consumers, and improved health and safety.

In the area of blockchain standardization, NIST is actively participating in consensus-based, documentary standard development efforts at both national and international levels.
For example, NIST participates in Accredited Standards Committee X9 (ASC X9) and INCITS, and will participate in the newly formed IEEE blockchain initiative. NIST participates as well in ISO Technical Committee 307 – Blockchain and Distributed Ledger Technologies.

Potential and Emerging Applications of Blockchain Technology

While financial organizations are likely to be the businesses most impacted by blockchains, many potential uses and opportunities for blockchain technologies exist beyond digital currency. For example, companies that need to maintain public records, such as holding a land title, marriage certificates, or birth records, can take full advantage of blockchains.

Blockchains also have strong potential for storing and recording supply chain records. A blockchain can record each step in a product's life: when it was created in a factory; when it was shipped and subsequently delivered to a store; and when a consumer purchased it.

New industries may also benefit from blockchain. Such industries include digital notaries seeking to prove that a person accessed a specific piece of information by recording its hash into the blockchain.

Conclusion

Blockchains are exciting technologies that have the potential to address real corporate and consumer needs using a strong and verified trust model. Much work still needs to be done to understand this technology, bring out its potential, and set the stage for markets to reward usable and secure implementations that meet real customer needs.

NIST will continue its research and development in the foundational cryptography that blockchains use. We will continue to learn from our research and continue to build collaborations with industry in the publication of guidelines. NIST is also continuing to work with international standards bodies that have started study groups and technical committees to initiate standards work for blockchains. This is an exciting time for blockchain technology, as it emerges into markets and sectors.

Thank you for the opportunity to testify on NIST's work regarding blockchain. I will be pleased to answer any questions you may have.

Charles H. Romine

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL, one of seven research Laboratories within the National Institute of Standards and Technology (NIST), has an annual budget of $150 million, nearly 400 employees, and about 200 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission, to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the Nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

Education:
Ph.D. in Applied Mathematics from the University of Virginia.
B.A. in Mathematics from the University of Virginia.

Chairman ABRAHAM. Thank you, Dr. Romine.

I now recognize Mr. Cuomo for five minutes to present his testimony.

TESTIMONY OF MR. GENNARO "JERRY" CUOMO, IBM FELLOW, VICE PRESIDENT BLOCKCHAIN TECHNOLOGIES, IBM CLOUD

Mr. CUOMO. Good morning, Chairman Abraham, Chairwoman Comstock, Ranking Members Beyer and Lipinski, and Members of the Subcommittee. My name is Jerry Cuomo, and I'm the Vice President for IBM Blockchain Technologies. And thank you very much for the opportunity to testify this morning.

Most people who've heard of blockchain associate it with the cryptocurrency Bitcoin. While they're related, it's important to understand that they're not the same. The potential uses for blockchain are far broader than cryptocurrency. We've engaged in more than 400 blockchain projects across supply chain, government, health care, transportation, insurance, chemical petroleum, and more. And from those experiences, we've developed three key benefits.

First, we believe that blockchain is a transformative technology that could radically change the way businesses and government interact. At the center of a blockchain is a shared immutable ledger. Each member of a blockchain network has an exact copy of the ledger as it updates over time. Transactions, once entered, cannot be changed. With this shared copy of the truth, time is saved because multiparty transactions could be now settled in real time. Cost is reduced because overhead is eliminated with businesses interacting directly. Risk is mitigated because the ledger acts as an immutable audit trail.

IBM and Maersk recently announced a joint venture to create an industrywide trading platform for ocean freight. Currently, a shipment of goods between ports can generate a sea of paperwork. Blockchain helps in real time track millions of shipping containers across the world with the potential to save billions of dollars and transform the shipping industry.

Our second belief is that blockchain must be open to encourage broad adoption, innovation, and interoperability. And for this reason, IBM is participating with over 180 industry players in the Hyperledger organization led by the Lennox Foundation. Only with openness will blockchain be widely adopted and spur innovation. IBM's collaborating with companies like SecureKey and the Sovrin Foundation on blockchain-based digital identity. Together, we are working to create a global ecosystem of blockchain identity networks backed by open standards where only the information that needs to be shared is shared with only those parties that have a need to know.

And we finally believe that blockchain is ready for business and government use today. A new breed of blockchain technology is now available. It meets four key requirements. First, it supports accountability, which is gained by known parties identified by cryptographic membership keys, entrusted data from an immutable ledger.

Next is privacy. While members are known to the network, transactions are only shared with those that have a need to know.

Third is scalability, handling an immense volume of transaction. A recent research paper demonstrated best of class and blockchain performance of more than 3,500 transactions per second.

And last but not least is security. With fault-tolerant algorithms, a network continues to operate even in the presence of bad actors or carelessness.

IBM is working with 12 major food companies, including Walmart, Unilever, and Nestle, applying our enterprise blockchain to rapidly trace food as it moves from farm to table, making it possible to quickly pinpoint the sources of contamination, reduce the impact of food recalls, and limit the number of people who get sick or die from foodborne illnesses.

Now, with those beliefs in mind, let me now turn to our recommendations to Congress. First, let's focus efforts on projects that can positively impact U.S. citizens and economic competitiveness. The Congressional Blockchain Caucus has already begun critical work on blockchain topics, including identity payments and supply chain. I recommend we use this work as the base to explore blockchain adoption, then use the knowledge gained to inform policy.

The second recommendation is to thoughtfully insert blockchain into projects already funded. Look for opportunities to fuel innovation in the broad ecosystem of U.S. businesses by encouraging blockchain projects as part of initiatives like the Small Business Innovation Research program.

And finally, we urge Congress and the Trump Administration, when considering regulatory policy, to recognize the difference between blockchain's use in new forms of currency from broader uses of blockchain to avoid consequences that stymie innovation. And please remember, blockchain is not Bitcoin.

Blockchain is ready for government. Now, let's get government ready for blockchain. I look forward to answering your questions and continuing the discussion. Thank you very much.

[The prepared statement of Mr. Cuomo follows:]

Gennaro (Jerry) Cuomo

IBM Fellow

Vice President, Blockchain Technologies

House Committee on Science, Space and Technology

Subcommittee on Oversight & Subcommittee Research and Technology

"Beyond Bitcoin: Emerging Applications for Blockchain Technology"

February 14, 2018

Introduction

Good morning, Chairman Abraham, Chairwoman Comstock, Ranking Member Beyer, Ranking Member Lipinski and Members of the Subcommittees.

My name is Jerry Cuomo, and I'm the Vice President for Blockchain Technologies, at IBM.
Thank you very much for the opportunity to testify this morning.

We at IBM believe that blockchain is a revolutionary technology. With blockchain we can reimagine many of the world's most fundamental business processes and open the door to new styles of digital interactions that we have yet to imagine.

You are wise to explore the science of blockchain technology – and its potential applications beyond cryptocurrency and financial technology – because blockchain has the potential to vastly reduce the cost and complexity of getting things done across industries and government.

Today, my testimony will share some key beliefs we hold at IBM based on our experience as an industry leader in blockchain. I'll also share some concrete examples that illustrate the transformative power of blockchain. Finally, I will include some recommendations for Congress and the Trump Administration that could ultimately help U.S. competitiveness and our citizens by preparing, advancing and applying blockchain in new ways – as I believe we should.

IBM's Blockchain Beliefs

Most people who have heard of blockchain associate it with the cryptocurrency Bitcoin. While they are related, it is important to understand they are not the same thing. Bitcoin is merely one example of a use of blockchain technology. Bitcoin operates with a network of anonymous participants. However, blockchain can also be used as a trusted network, using permissioning, to handle interactions between known parties. As an analogy, the internet like blockchain is a transformational building block for many types of communication, Bitcoin and other forms of cryptocurrency are but one use of blockchain, just as social media is but one use of the internet.

We have engaged with clients in over 400 blockchain projects across supply chain, financial services, government, healthcare, travel and transportation, insurance, chemicals and petroleum, and more.

This experience has led us to develop three key beliefs that I'd like to share with you today:

1. Blockchain is a transformative technology.
2. Blockchain must be open.
3. Blockchain is ready for business and government use TODAY.

Blockchain Belief #1 – Blockchain is a transformative technology

First and foremost, blockchain is changing the game. In today's digitally networked world, no single institution works in isolation.

At the center of a blockchain is this notion of a shared immutable ledger. You see, members of a blockchain network each have an exact copy of the ledger. New entries in the ledger are propagated throughout the network. Therefore, all participants in an interaction have an up-to-date ledger that reflects the most recent transactions and these transactions, once entered, cannot be changed on the ledger.

Blockchain's power to transform is that it enables co-development of a shared copy of the truth. And with this, what a group can achieve together far exceeds what any individual member can achieve by themselves.

Now let me tell you how blockchain actually changes the game.

1. **Time** is saved because multi-party transactions can settle immediately avoiding exhaustive reconciliation that often takes days or even months.
2. **Cost** is reduced because business-to-business processing eliminates overhead caused by "middle-men".
3. **Risk** is mitigated because the ledger acts as an immutable audit trail greatly reducing the chances for tampering and collusion.

This leads to my first example, IBM and Maersk, the world's largest shipping company, recently announced our intention to form a joint venture to create an industry-wide trading platform for the ocean freight industry. This industry accounts for 90 percent of goods shipped in global trade. Currently, one shipment of goods between two ports can generate a sea of paper and information exchanges between 30 different public and private organizations. The joint venture will use blockchain to help track in real-time millions of shipping containers across the world by providing a trusted, tamper-proof, cross-border system for digitized trade documents. By having a shared blockchain ledger, companies can reduce the time spent resolving disputes, finding information, and verifying transactions, leading to quicker settlement. When adopted at scale, the solution has the potential to save billions of dollars. This is the transformative power of blockchain applied to the shipping industry.

And blockchain technology provides the springboard for an even broader spectrum of innovation. Let me just take a moment to tell you about a project from the IBM research lab. Uniquely identifying a physical asset such as a type of a diamond, petroleum, or a manufactured part as a corresponding digital asset in a blockchain network is an interesting challenge; verifying authenticity is important.

These physical products travel through many hands and companies before reaching their final destinations. At any point along the supply chain, a valuable physical asset could have been swapped with a counterfeit one. To help ensure provenance on the blockchain, at IBM Research, we invented a

smartphone-based artificial intelligence technology used to scan the high value item. Using light spectral analysis to capture the microscopic properties, viscosity and other identifiers creates a digital fingerprint that can be used to verify authenticity and avoid counterfeiting documents or fake substitute products.

Blockchain Belief #2 – Blockchain must be open

For blockchain to fulfill its potential, it must be based on non-proprietary technology. Doing so will encourage broad adoption and ensure the compatibility and interoperability of systems. Specifically, this enterprise-ready blockchain must be built using open source software, with a combination of flexible licensing terms and strict governance by an open community, meaning there is no one controlling organization that governs the direction of the project and no lock-in to one vendor. Much as we have seen with the internet, only with openness will blockchain be widely adopted and enable innovation.

For this reason, IBM is participating with over 180 industry players in the Hyperledger organization, led by the Linux Foundation. Hyperledger is a collaborative open-source, open-standards and open-governance effort created to advance cross-industry blockchain technologies for business and government.

For example, IBM is collaborating with companies like SecureKey and the Sovrin Foundation on blockchain-based digital identity. Together, we are working to create a global ecosystem of blockchain identity networks backed by global standards. These standards are defining mechanisms by which only the information that needs to be shared is shared with only those parties that need to know. With blockchain identity theft and fraud can be significantly reduced while at the same time increasing the effectiveness of Know-Your-Customer and Anti-Money Laundering efforts, doing so in a more cost-effective way. We can not only make it harder for criminals to impersonate someone, but in the event of a data breach, we can recover quickly. Unlike a social security number, blockchain-backed decentralized identifiers can easily be revoked and reissued if ever stolen or compromised.

Blockchain Belief #3 –Blockchain is ready for business and government use TODAY

Not all blockchain technology is created equal. For broad business and government use, enterprise blockchain technology is now available that solves four fundamental requirements: *accountability, privacy, scalability and security.*

Accountability means the participants transacting in a network, and the data they are transacting on, are both known and trusted. In an enterprise ready blockchain, participants are known and are identified by membership keys. The data can be trusted because transactions committed to the ledger are immutable – such that they cannot be removed or changed by the actions of a single party.
With this accountability the network is auditable allowing members to follow and adhere to existing government regulations like HIPAA and GDPR.

Even though participants are known, they must be able to transact with *privacy* on the network. Businesses require that both their transaction data and the transactions themselves are confidential. An enterprise blockchain enables confidential communications when information is not desired to be shared with the entire network.

Computer systems and networks must be architected to have the *scalability* to handle an immense volume of transactions. Because trust in an enterprise blockchain network is not built through anonymous "mining" (as is done in Bitcoin), transaction performance has been demonstrated at levels needed for high volume throughput. A recently published research paper demonstrated one such enterprise blockchain performance at a best-of-class rate of more than 3500 transactions per second (https://arxiv.org/abs/1801.10228).

The need for *security* continues to be illuminated by breaches in the news every month. As much as everyone tries, it's impossible to eliminate all people with malicious intent or sloppy actions. A enterprise blockchain network is fault tolerant, implementing algorithms like crash and byzantine fault tolerance that allow a network to continue to operate even in the presence of bad actors or carelessness.

These four requirements are delivered today in the Hyperledger Fabric, one of the popular blockchain frameworks from the Hyperledger project. It now serves as the basis for over 40 active blockchain networks that are running on the IBM Blockchain Platform.

For example, every year 400,000 people around the world die from foodborne illness. With the advent of global supply chains, it's very difficult to trace contaminated food back to the source, as we witnessed with the recent e. Coli outbreak that sickened 60 people and took 2 lives over a period of 6 weeks. IBM is working with twelve major food companies – including Walmart, Unilever, and Nestle – applying our enterprise blockchain to rapidly trace food as it moves from farm to table, showing how blockchain has the potential to help keep entire populations healthier. Blockchain makes it possible to quickly pinpoint the source of contamination, reduce the impact of food recalls and limit the number of people who get sick or die from foodborne illness.

Recommendations for Congress and Trump Administration

We are working with many government entities in activities for the adoption and use of blockchain technology: from U.S. agencies such as the FDA, CDC and OPM exploring how blockchain can reduce complexity to the Smart Dubai initiative to trusted digital identity projects in Canada. U.S. companies are leading in blockchain technology development while U.S. government agencies like NIST actively engage in blockchain standards exploration. While blockchain remains a team sport, there is an opportunity for the United States to build upon its momentum to lead blockchain by doing. I'd like to make a few recommendations to help Congress and the Trump Administration along this path.

First, we should focus our efforts on projects that can positively impact U.S. economic competitiveness, citizens and businesses. The Congressional Blockchain Caucus, led by Reps. Jared Polis and David Schweikert, has already begun this critical work. The Blockchain Caucus is working to collect information on blockchain projects that could help individuals securely establish their identity, make key payments -- such as tax payments – and revolutionize supply chains. This work should fuel initiatives that can make a meaningful difference in citizens lives like the digital identity, food safety, and transport supply chain examples we discussed as well as other potential uses cases like land registration, taxation and more. I recommend we explore blockchain adoption and use with these citizen and business-focused projects first. Then, use the knowledge gained to inform policy and regulation in different blockchain technology

implementations going forward. In the same spirit we commend the House for passage of the Perkins Act, that will facilitate government, academia, and private sector collaboration in order to advance skills building.

Second, thoughtfully inserting blockchain in appropriate projects already funded would help ensure we stay at the forefront of this transformative technology. Consider blockchain technology as an enabler to lower cost, time and risk in currently budgeted projects. In addition, look for opportunities to fuel innovation in the broader ecosystem of U.S. businesses by encouraging blockchain projects as part of the Small Business Innovation Research (SBIR) program that is part of existing research budgets in a number of agencies today.

Finally, and perhaps most importantly, recognize the difference between blockchain's use in new forms of currency from broader uses of blockchain when considering regulatory policy. Carefully evaluate policies established regarding cryptocurrencies to ensure that there will not be unintended consequences that stymie the innovation and development surrounding blockchain. A policy that has not been carefully vetted could risk inhibiting the U.S. leadership position.

Blockchain is ready for government, now let's get government ready for blockchain. We at IBM stand ready to help provide the analysis of any such policies and would be happy to work collaboratively with Congress to ensure the continued expansion and success of blockchain.

Conclusion

Thank you for the opportunity to discuss such an important topic for our present and our future.
In summary, at IBM we believe that:

1. Blockchain is a transformative technology: It enables the many to achieve more than is possible by the one.
2. Blockchain must be open: Only then will blockchain be widely adopted as a springboard for innovation.

3. Blockchain is ready for business and government use TODAY: it provides accountability, privacy, scalability and security.

At IBM, we are actively working to ensure businesses and governments are thoughtfully implementing this technology and we believe the United States has an opportunity to lead in this space.

I will look forward to answering your questions and continuing this discussion. Thank you.

Gennaro (Jerry) Cuomo

IBM Fellow, Vice President Blockchain Technologies

Jerry Cuomo is recognized as one of the most prolific contributors to IBM's software business, producing products and technologies that have profoundly impacted how the industry conducts commerce over the world-wide-web, while dramatically improving the consumer experience.

Jerry has exhibited a repeating pattern of breakthrough innovations in software design, engineering and business strategy, across IBM's most financially successful and industry recognizable software product offerings.

Jerry holds the prestigious title of IBM Fellow, which is the highest technical position at IBM, with only 300 Fellows having been named in the 106 years of IBM's existence.

Jerry has pioneered emerging technology projects in the areas of Blockchain, API Economy, Mobile computing, Cloud computing, Web Application Servers, Integration Software, Java, Instant Messaging Software, filling over 60 US patents across these areas.

Jerry is most recognized as one of the founding father of WebSphere Software, whose innovations defined WebSphere as the Industry leading Application Server currently serving over 80,000 customers. WebSphere re-imagines how business, governments and citizens get work done using the Internet.

Cuomo's inventions in web server security, performance, scalability and availability are the reasons why many of the world's most visible institutions are able to securely conduct commerce over the world wide web.

Jerry's most visible patent is the first use of the "Someone is typing..." indicator found in instant messaging applications. This invention is used by billions of users around the world every day, via their iPhones, Microsoft's Messenger, and IBM's Sametime.

Today, Jerry is leading the definition of IBM's Blockchain strategy and offerings. Jerry and team have illustrated how blockchain can revolutionize business and redefine companies and economies.

In March 2016, Jerry was called upon by the US Government as an expert witness to testify to US Energy and Commerce Committee on Digital Currency and Blockchain. During his testimony Jerry urged the Obama administration to adopt Blockchain as a primary means to protect citizen identity and to enhance national security. His testimony can be seen on YouTube and is often referred to in social media.

Chairman ABRAHAM. Thank you, Mr. Cuomo.

Mr. Yiannas, I recognize you now for five minutes for your testimony.

TESTIMONY OF MR. FRANK YIANNAS,
VICE PRESIDENT OF FOOD SAFETY, WALMART

Mr. YIANNAS. Chairman Abraham, Comstock, and Members of the Committee, on behalf of Walmart, I want to thank you for the invitation to testify here today on the use of blockchain technology and its potential applications beyond cryptocurrency and finance. My name is Frank Yiannas, Vice President of Food Safety for Walmart, the world's largest retailer.

Walmart helps people around the world save money so they can live better. Each week, more than 260 million customers visit our nearly 12,000 stores in 28 countries or shop with us on our e-commerce platforms. With fiscal revenue in 2017 of $485.9 billion, grocery sales accounted for approximately 56 percent of those revenues in our U.S. formats. Operating in that many formats and in so many countries presents us with a daunting challenge and an important responsibility. Our customers rely on Walmart as their trusted buying agent.

Too often people talk about a food chain, but it's not a linear chain at all. Today, the way we get our food from farm to table is a food system, and it's a complex network of many interdependent entities. While today's food system provides consumers with benefits, it also can present challenges. For example, the output of one contaminated ingredient could end up in thousands of products. We saw evidence of this during the peanut butter outbreak in 2008 and more recently with flour in 2016.

Blockchain is the distributed decentralized digital ledger that makes it possible to store and share data across complex networks in a more secure, effective, and democratic way. Features of immutability, consensus, and a complex network without a single authority allow the blockchain system to create one version of the truth and to rapidly scale trust, which is good for business.

Today, many involved with food still use paper-based systems to manage records, and even if they capture that information in digital form, that data is often in disparate systems that don't speak with each other. Being able to track how food flows from farm to table can be a very difficult and lengthy task. Each participant discloses their products path one step forward and one step back. Regulators and retailers have to take that data and piece it together to find or manually determine the origin of a problem. For example, in 2006 in a nationwide outbreak of E. coli here in the United States, it took regulators two weeks to conduct the traceback and determine the exact source of the contamination. We've seen similar timelines and outcomes in more recent food safety squares.

In 2017, Walmart and IBM conducted two proof-of-concepts using blockchain for food traceability. For one pilot here in the United States, we decided to track the journey of mangoes from farm to store. That journey includes several stops along the way before they arrive in our stores as packages of sliced mangoes. For the test, we work with supplier and their supply chain to capture food traceability attributes onto the blockchain. We captured informa-

tion about the mangoes, where were they grown, how were they harvested, how did the travel, and so on. At the conclusion of that pilot, we demonstrated that we could accelerate tracing the origin of sliced mangoes back from our stores to a farm down from 7 days to 2.2 seconds. That's food traceability at the speed of thought.

As the food system is global in nature, we also conducted a second pilot in China, and it involved pork, one of the region's most important animal proteins. With the use of blockchain technology, at the store a case of pork could be scanned with a simple QR code and tracked back to the farm from which it came. We were also able to pull up digitized authentic veterinary records, increasing our confidence in the authenticity of that product.

After our successful pilot with IBM, we rapidly mobilized with a group of influential companies to share our results, and we invited them to participate in additional testing. Today, we have a coalition of 11 foundation partners comprised of Walmart suppliers and peers in retail, all working together to further test blockchain. We seek a collaborative solution rather than each company trying to create one on their own. We're also placing emphasis on the importance of blockchain systems being interoperable and based on existing industry standards. Walmart and IBM the foundation partners have moved rapidly to scale, test, and learn, and Walmart is now testing blockchain on dozens of selected food items.

While we've been working on food traceability, we believe blockchain could lay the groundwork for other benefits beyond food traceability such as optimizing supply chains and reducing food waste. Our ultimate goal is food transparency. By getting rid of the anonymity that exists in the food system today, we believe the blockchain could help shine a light on every step of how that food is produced and travels. This enhanced transparency will result in a safer, more efficient, and sustainable food system so that people can live better.

Thank you for the opportunity to share our thoughts on blockchain applications in food, and we look forward to answering any of your questions.

[The prepared statement of Mr. Yiannas follows:]

U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight, and;
Subcommittee on Research and Technology

February 14, 2018

Hearing on:

"Beyond Bitcoin: Emerging Applications for Blockchain Technology"

Testimony of Frank Yiannas
Vice President, Food Safety
Walmart Inc.

Chairmen Abraham and Comstock, Ranking Members Beyer and Lipinski, and members of the committee:

Introduction:

On behalf of Walmart Inc., (Walmart) I thank you for the invitation to testify here today on the use of blockchain technology and its potential applications beyond cryptocurrency and finance.

My name is Frank Yiannas, and for the past ten years I've served as the Vice President of Food Safety for the world's largest retailer, Walmart, where I am responsible for all food safety compliance as well as other public health programs. Prior to joining Walmart in 2008, I was the Director of Safety and Health for Disney where I worked for 19 years. I am also the author of two books on Food Safety Culture and Behavior.

Company Background:

Walmart helps people around the world save money and live better whenever they shop in our stores or online with us. Each week, more than 260 million customers visit our nearly 12 thousand stores in 28 countries or shop with us on our e-commerce websites. With fiscal year 2017 revenue of $485.9 billion, Walmart employs approximately 2.3 million associates worldwide.
In regards to food, our grocery sales accounted for approximately 56% of our revenues in our Walmart U.S. format last year.

Food System Complexities:

Operating that many formats in so many countries around the world also presents us with a daunting challenge. Our customers rely on Walmart to act as their trusted buying agent. They trust – and indeed expect – that we know as much as we can about the food we sell in our stores and online. With that responsibility, we are always looking for ways to advance food safety and improve public health.

Too often people talk about the "food supply chain", but in reality, it isn't a linear chain at all. Today, the way we get our food from farm to table, the "food system", has evolved into a complex network interdependent on many entities. And while there is no question that today's food system has provided consumers with a more diverse, convenient, and economical source of food, it also, at times, presents new challenges.

For example, in today's food system, the output from one ingredient producer could end up in thousands of products on a grocery store shelf. We saw evidence of this during the peanut butter outbreak in 2008 and more recently with flour in 2016.

This complexity is one of many reasons we were looking for a technological solution to help us achieve enhanced food traceability and transparency.

What is Blockchain and Why is Important to the Food System?

Blockchain is a distributed, decentralized digital ledger that makes it possible to store and share digitized data across complex networks in a more secure, effective, and democratic way.

Using advanced cryptography and consensus algorithms, a blockchain protocol takes data inputted by a network participant as a block and converts it into a unique alpha-numeric sequence called a hash, which can be permissioned and shared with other actors in the system in a secure and trusted way.

Features of immutability, consensus, and the ability to conduct transactions in a complex network without a central authority, allow blockchain systems to create **one version of the truth and rapidly scale TRUST,** which is good for business.

Coming back to food, in today's food system, many participants involved with producing and distributing food still use paper-based systems to manage records. Even if they capture information in digital form, the data is often in disparate systems that do not speak with each other. Therefore, being able to track how food and food ingredients flow from farm to table can be a very difficult, labor intensive and lengthy task. Each participant in the continuum must disclose their product's path "one step forward and one step back." Regulatory bodies and retailers must take that data and piece it together manually to determine the source of an issue.

For example, in 2006, in a nationwide outbreak of E coli 0157:H7 linked to bagged spinach in the United States, consumers were advised, rightfully so, to avoid eating bagged spinach, regardless of brand, until the exact source could be identified. Retailers and restaurants pulled all bagged spinach, regardless of source, off of store shelves and menus. It took regulators two weeks to conduct the trace back and determine the exact source of the outbreak. When it was all said and done, the outbreak was linked to only one producer, one day's production, and one lot number. It took the spinach industry many years to regain consumer confidence and get back to previous levels of production and sales.

This is not an isolated scenario. We have seen similar timelines and outcomes in other food scares.

In 2008, we saw weakness in the ability of many food suppliers to quickly trace and report whether or not contaminated peanut paste from a single facility was used in their products. In the end, it took some suppliers up to two months to identify that the potentially contaminated peanut paste was used as an ingredient in almost 4,000 different SKUS (stock keeping units), ranging from peanut butter crackers to chocolates and pet treats.

Walmart's Food Traceability Pilots Powered by Blockchain

In early 2017, Walmart and IBM conducted two proofs of concept that successfully demonstrated that blockchain technology could provide a viable solution to track and verify food from origin to our stores with speed, accuracy, and precision.

- **Sliced Mangoes** - for one proof of concept conducted here in the United States, we decided to do the pilot with sliced mangoes sold in our Stores. In this hemisphere, mangoes tend to be grown on small farms in Central and South America. Once those mangoes start ripening each season, packing crews will harvest the mangoes where they will be shipped to a packing facility where they are washed, hot water treated, and boxed. Those mangoes will make multiple stops before they arrive as packages of sliced mangoes in our stores. The life of a mango is a pretty complicated and amazing journey.

  For the mango proof of concept, we worked with a supplier and their supply chain to capture food traceability data attributes, along with other data attributes, into the blockchain. We captured information about where the mangoes were grown, when they were harvested, how they traveled, and so on.

  At the conclusion of the pilot, we were able to demonstrate that our ability to trace the origin of sliced mangos from our stores back to the farm could be improved **from 7 days** using traditional methods **down to 2.2 seconds** by using blockchain platforms. That's "food traceability at the speed of thought."

- **Pork in China** - as the food system is global in nature, our second proof of concept was conducted in China and it involved pork, one of the region's most important animal proteins. It also focused on a growing concern of the grocery industry, economically motivated adulteration, also commonly referred to as food fraud. Proving that this technology could be used to strengthen confidence in the authenticity of food, whether it is species substitution or a product claim, such as organically grown, was also important to us.

  With the use of blockchain technology, not only could the pork be tracked from a single Walmart Store back to the farm, it also increased assurance of the authenticity of the product and its records could be accessed as well. At the store, a case of pork could be scanned with a simple QR code to pull up digitized authentic production and veterinary records from the corresponding farm where that animal was raised.

Beyond Traceability – Food Transparency

Enhanced traceability is one of the many reasons why we are interested in blockchain technology. However, we believe blockchain could enable more than traceability. It could lay the groundwork for other benefits. Let me mention just a few:

- **Optimizing Supply Chains** – small improvements in supply chains can yield huge benefits. Blockchain technology as the basis for a new information highway, coupled with Artificial Intelligence and the Internet of Things (IoT), could enable instant access to large amounts of data and insights that could result in a safer, more efficient, and sustainable food system.

- **Reducing Food Waste** – one third of all food produced goes to waste. One of the outcomes of a smarter food system could be enhanced food flow, allowing fresher product to reach consumers and reducing food waste at home and along the entire food continuum.

- **Enabling Transparency** – today's customer expects more from their food system. Customers want to know more about their food. Where did it come from? Was it sustainably grown? Blockchain could serve as the foundation to capture this information and ultimately make it available to the customer, resulting in enhanced consumer confidence and trust.

Democratizing the Benefits – Creating Shared Value

One last concept that we would like to emphasize is how blockchain technology is different than many current digital protocols. Its benefits are decentralized and more democratic. In many of today's digital systems, data tends to exist in silos and is owned by a central authority. For example, a retailer might ask their suppliers to disclose information about their suppliers, where they source ingredients and more. Suppliers that disclose such information often have to do similar disclosure activities in other retailers' systems that they do business with, resulting in redundancies and inefficiencies. Moreover, sometimes, they never benefit from seeing any insights gained as a result of such data disclosure.

In contrast, in a permissioned blockchain system, the data is shared among system participants and it allows everyone to benefit and gain value. For example, farmers can benefit from not having their unaffected crops they grow inaccurately implicated in overly cautious product withdrawals. Food processors often get blamed when products do not meet shelf-life, when in reality it might be temperature abuse that occurred somewhere else in the distribution continuum.

Therefore, we believe blockchain will help democratize the benefits of digitizing data and allow the entire food system to get smarter together.

Expanding, Testing, and Scaling Across Multiple Companies

After our successful proof of concepts, Walmart and IBM contacted leaders of some of the most influential food companies to share our results, and invite them to participate in additional testing of blockchain applications. Today, we have a coalition of 11 Foundation Partners comprised of Walmart suppliers and peers in retail including: Walmart, Kroger, Wegmans, Tyson, Driscolls, Nestle, Unilever, Danone, McCormick, Dole, and Golden State Foods, all committing to work together in testing the technology.

We believe that partnership is critical in order to create an open, collaborative solution that works for everyone, rather than each company attempting to create solutions in isolation. Many of the inefficiencies we experience during outbreak investigations are due to utilization of different data formats in separate systems that don't speak to each other. Therefore, we are placing an enormous emphasis on the importance of interoperability of blockchain systems and the use of existing industry standards. Where those standards don't exist, we will work with industry leaders and associations to

create them. Without the utilization of standards in an open system, we won't be able to realize the gains in speed and efficiency that we intend to make.

Walmart, IBM, and the Foundation Partners have moved rapidly to scale and implement blockchain enabled traceability and we are now testing it on dozens of strategically selected SKUs.

Conclusion

Again, our ultimate goal is food transparency. By getting rid of the anonymity that exists in the current food system, blockchain technology will shine a light along every step of the way in how food travels and get produced. This enhanced transparency will lead to greater accountability and, ultimately, help create a safer, more efficient, and sustainable food system, so that people can save money and live better.

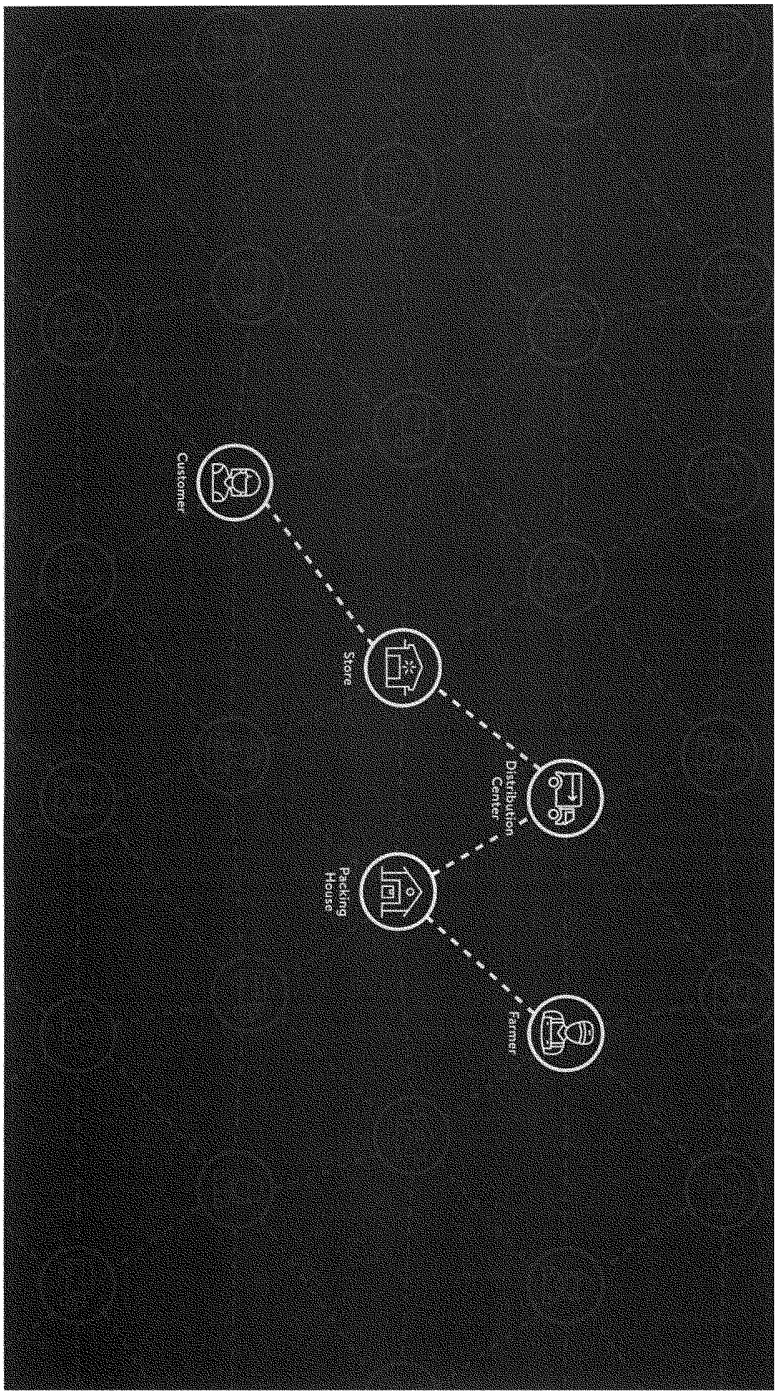
Thank you for the opportunity to share our thoughts on blockchain applications in the food system, and I look forward to answering any questions you may have.

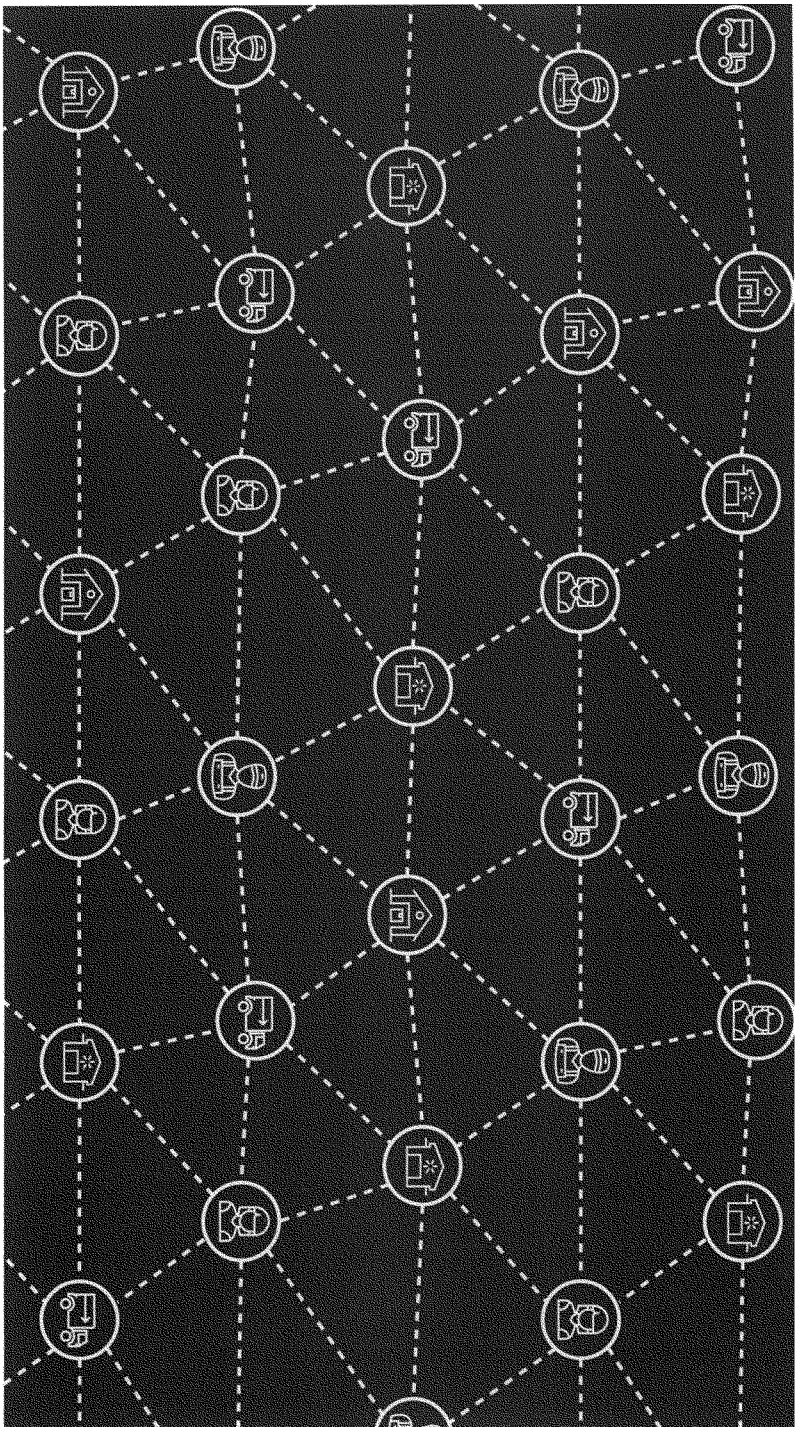
Walmart

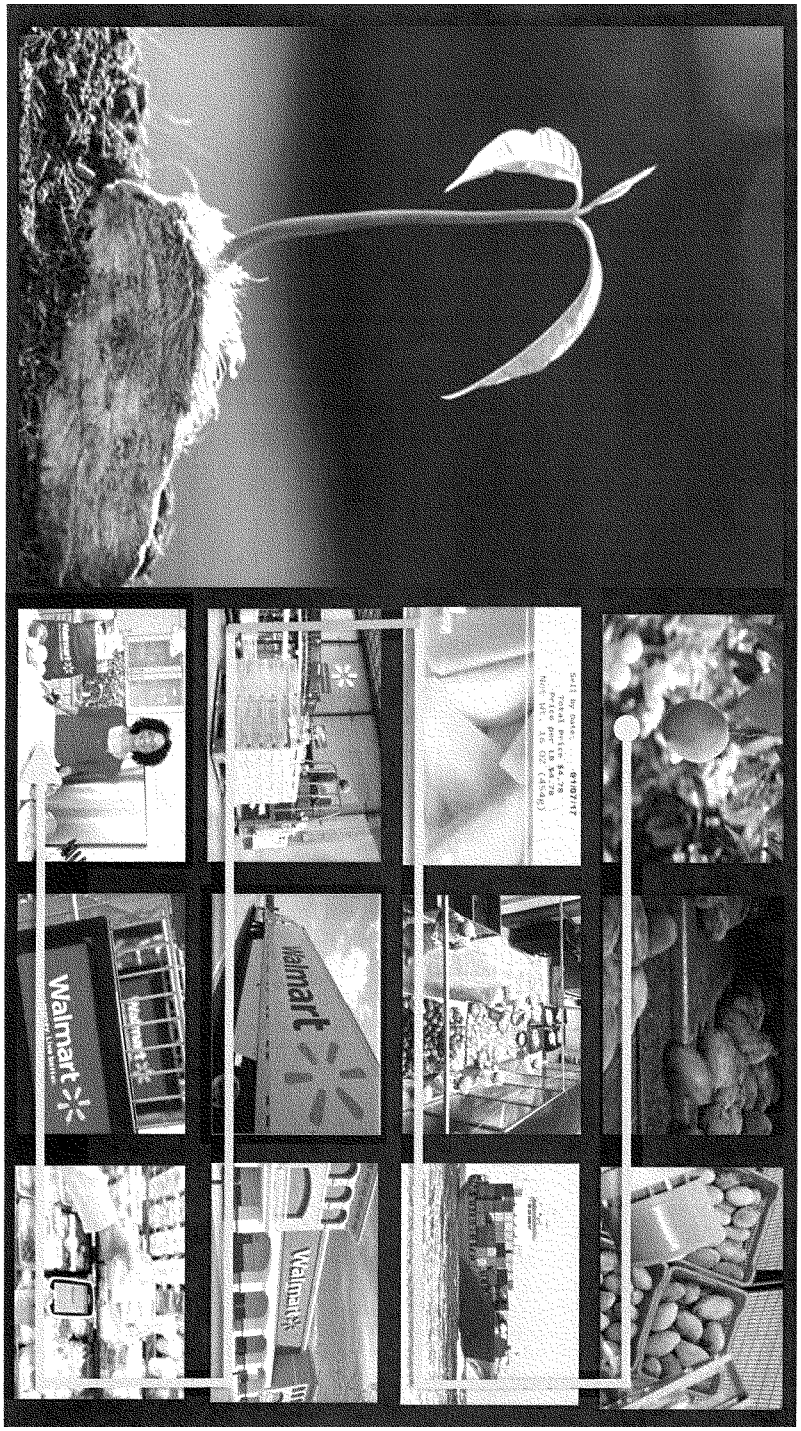
FRANK YIANNAS | Vice President – Food Safety

As Vice President of Food Safety, Frank Yiannas oversees all food safety, as well as other public health functions, for the world's largest food retailer, Walmart, serving over 200 million customers around the world on a weekly basis. Prior to joining Walmart in 2008, Frank was the Director of Safety & Health for the Walt Disney World Company, where he worked for 19 years. In 2008, Frank was given the Collaboration Award by the U.S. Food and Drug Administration. He is the 2007 recipient of the NSF International Lifetime Achievement Award for Leadership in Food Safety and the 2015 Industry Professional Food Safety Hero Award by STOP Foodborne Illness. Frank is also a Past President of the International Association for Food Protection (IAFP) and a Past Vice-Chair of the Global Food Safety Initiative (GFSI). He is also an adjunct Professor in the Food Safety Program at Michigan State University, and in 2017 was awarded the MSU Outstanding Faculty Award. He is the author of the books, *Food Safety Culture, Creating a Behavior-based Food Safety Management System,* and *Food Safety = Behavior, 30 Proven Techniques to Enhance Employee Compliance*, by Springer Scientific. Frank is a Registered Microbiologist with the American Academy of Microbiology. He received his BS in Microbiology from the University of Central Florida and his Master of Public Health (MPH) from the University of South Florida.

[Slides]






Walmart
Walmart
Walmart
Walmart
Walmart

Chairman ABRAHAM. Thank you, Mr. Yiannas.

Mr. Wright, you have five minutes, sir.

TESTIMONY OF MR. AARON WRIGHT, ASSOCIATE CLINICAL PROFESSOR AND CO-DIRECTOR OF THE BLOCKCHAIN PROJECT, BENJAMIN N. CARDOZO SCHOOL OF LAW

Mr. WRIGHT. Chairman Abraham, Ranking Member Beyer, Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittees, thank you for the opportunity to testify before you today. I hope my testimony will provide further insight on the potential and risks of blockchain technology, particularly with respect to next-generation public and open blockchains such as Ethereum. I also hope my testimony will spur these committees to support policies to continue to position the United States as a global leader in this technology.

My name is Aaron Wright, and I am a law professor, writing and teaching primarily in the area of technology law. Over the past four years, I've dedicated my academic efforts to researching and developing blockchain technology, writing about policy issues associated with blockchain technology, and counseling blockchain technology projects. As part of those efforts, I'm developing a project called OpenLaw, in conjunction with ConsenSys, which allows anyone to create smart legal agreements that leverage blockchain technology; serving as an advisor to an early seed company BlockApps; chairing the Legal Industry Working Group of the Enterprise Ethereum Alliance; and helping to organize the Brooklyn Project, a collaborative industry effort to develop sensible regulatory standards for blockchain technology.

As you've heard from the other witnesses, blockchains are useful for far more than just virtual currencies like Bitcoin. They're underpinning an array of online services that seek to use the technology to store information. However, I also wanted to emphasize that they're also being used to run potentially autonomous computer processes called smart contracts. Both blockchains and smart contract could potentially impact a range of industries in the United States, improving commercial activity.

As we've seen over the past two years, blockchains are poised to transform capital markets. Blockchain technology is being explored to improve the efficiency of traditional financial services, creating digitized financial agreements that are settled and cleared on a bilateral basis with less of a need for third-party administration.

Perhaps of greater long-term importance, blockchains are securing scarce digital assets, often referred to as tokens, which parties transfer using smart contracts in a secure and largely irreversible way, with less of a need for centralized intermediaries. These tokens are powering new forms of crowdfunding, often referred to as token sales, and serve as a potentially potent new tool for entrepreneurs to build powerful new network-based technology platforms. The sale of these tokens ultimately could democratize access to capital and help spur innovation throughout the United States, building a fairer society.

The impact of blockchain technology is spreading to the legal industry and other industries heavily reliant on contractual arrange-

ments to structure business activity. By using blockchain-based smart contracts to memorialize payment and performance obligations and recording agreements on a blockchain, we may move soon beyond an era with contracts written in natural language to an era where we have agreements written in code.

Outside of the private sector, governments across the globe, including China, Japan, and the E.U. are exploring blockchain technology in more detail and looking to see whether the technology can secure and manage critical public records and exploring whether blockchains can improve government procurement and taxation processes. Through these efforts, it's conceivable that blockchains could anchor global and transnational systems, including university-accessible secure identification systems that could prevent abuses like human trafficking, secure voting systems, transnational land and IP registries, and global marketplaces available to all.

Extending beyond governmental services, blockchains are increasingly being explored to control devices and machines in a secure manner. If these attempts prove successful, blockchains could foster a new era of machine-to-machine and machine-to-person interactions and commerce.

Despite these opportunities, however, blockchains have a number of risks. The disintermediated and transnational nature of public blockchains makes them difficult to govern and change, and they can be used to coordinate socially unacceptable and criminal conduct. Of greatest present concern, a slate of more anonymous new digital currencies are making it progressively easier to avoid anti-money laundering and other financial rules related to payment systems. Entrepreneurs are using blockchain technology to sell tokens in ways that avoid security law requirements, often with the aid of complicit lawyers that emphasize form over substance.

Cryptocurrency exchanges for these digital goods, particularly those located abroad, appear to have implemented weak measures to prevent abusive trading practices, and new decentralized marketplaces and exchanges are emerging, which could operate without any centralized operator policing the network for illegal activity.

Due to the nascent nature of blockchains, the U.S. Government has a unique ability to shape the development of the technology going forward. As the guiding principle, however, it's my hope that the United States proceeds with thoughtful technology-neutral regulation that permits the exchange of blockchain-based assets, particularly those that are consumer-focused without undue regulation that enables parties to build blockchain-based protocols to address some of the technical limitations described by the other witnesses without fear of regulatory scrutiny and provides a predicable and simple legal environment that protects consumers without insulating entrenched market participants.

To support these research and policy goals, I'd encourage Congress to contemplate commissioning a National Blockchain Commission that would aim to cement America's technological standing and increase economic growth and innovation. The commission could explore ways to invest in blockchain-based research through prizes or otherwise, devise common principles to guide the federal approach for regulating blockchain technology, hold hearings, con-

duct research, and make recommendations to industry, the executive branch, and Congress. Through the above approach, we can ensure that the United States remains the best place to develop, launch, and grow blockchain-based projects, and we can implement sensible and necessary guardrails to guide blockchain's development.

Thank you very much for the opportunity to testify, and I look forward to any questions you may have.

[The prepared statement of Mr. Wright follows:]

CARDOZO LAW

BENJAMIN N. CARDOZO SCHOOL OF LAW • YESHIVA UNIVERSITY

Aaron Wright
Associate Clinical Professor of Law
Co-Director, Cardozo Blockchain Project

(212) 790-0420
aaron.wright@yu.edu

Testimony Before the Subcommittee on Oversight and
Subcommittee on Research and Technology

"Beyond Bitcoin: Emerging Applications for Blockchain Technology"

Aaron Wright
Associate Clinical Professor
Co-Director of Cardozo Blockchain Project
Wednesday, February 14, 2018

"Blockchain's Opportunities and Risks"

Chairman Abraham, Ranking Member Beyer, Chairwoman Comstock, Ranking Member Lipinski, Chairman Smith, Ranking Member Johnson, and members of the Oversight and Research and Technology Subcommittees, thank you for the opportunity to testify before you today. I hope my testimony will provide further insight on the potential and risks of blockchain technology, particularly with respect to next-generation public blockchains such as Ethereum. I also hope that my testimony will spur this Committee to increase funding for basic research of blockchain technology within the United States and encourage Congress to increase its exploration of the technology in line with the current efforts of other leading jurisdictions.

My name is Aaron Wright, and I am a law professor, writing and teaching primarily in the area of technology law. Over the past four years, I have dedicated my academic efforts to researching and developing blockchain technology, writing about policy issues associated with blockchain technology, and counseling blockchain technology projects. As part of those efforts, I am: (1) developing an academic project called OpenLaw, in conjunction with ConsenSys, which enables anyone to create "smart" legal agreements that leverage blockchain technology;[1] (2) serving as an advisor of a private blockchain company BlockApps;[2] (3) chairing the Legal Industry Working Group of the Enterprise Ethereum Alliance; and (4) helping to organize "The Brooklyn

[1] More specifically, OpenLaw enables anyone to model all or parts of a legal agreement using a domain specific language developed for lawyers. Any agreement created on OpenLaw is stored on the Ethereum blockchain and can call Ethereum-based smart contract. *See* OpenLaw.io, https://www.openlaw.io.
[2] BlockApps enables developers to build blockchain applications on top of a customized permissioned private blockchain or a public blockchain. *See* BlockApps, https://blockapps.net/.

Project," a collaborative industry effort to develop sensible regulatory standards for blockchain technology.[3]

Blockchains constitute a new infrastructure for the storage of data and the management of software applications, decreasing the need for centralized middlemen. While databases often sit invisibly behind online services, their significance cannot be understated. Databases serve as a backbone for every platform, website, app, or other online service. Up to this point, databases have been for the most part maintained by centralized intermediaries, such as large Internet companies or cloud computing operators. Blockchains are beginning to change this dynamic, powering a new generation of disintermediated peer-to-peer applications, which are less dependent on centralized control.

Blockchains blend together several existing technologies, including peer-to-peer networks, public-private key cryptography, and consensus mechanisms to create what can be thought of as a highly resilient and tamper-resistant database where people can store data in a transparent and non-repudiable manner and engage in a variety of economic transactions pseudonymously.[4]

More advanced blockchains, most notably Ethereum, also integrate decentralized computing systems enabling parties to write and deploy computer processes known as "smart contracts."[5] These programs are stored on a blockchain and are executed by multiple members of a blockchain's underlying peer-to-peer network, creating computer processes that are potentially autonomous and difficult to shut down once deployed.

While complex, public blockchains exhibit a set of core characteristics that differ from earlier data structures. Blockchains are disintermediated and often transnational. They are resilient and resistant to change and enable people to store non-repudiable data, pseudonymously, in a transparent manner. Most—if not all—blockchain-based networks feature market-based or game-theoretical mechanisms for reaching consensus, which can be used to coordinate people or machines. These characteristics, when combined, enable the deployment of autonomous software and explain why blockchains serve as a powerful new tool to facilitate economic and social activity that otherwise would be difficult to achieve.[6]

Importantly, for purposes of this hearing, blockchains are useful for more than just virtual currencies, like Bitcoin. They are underpinning an array of online services that seek to use the technology to store information and run computer processes in areas that could potentially impact a range of industries in the United States. I will highlight some use cases here:

As we have seen over the past two years, blockchains are poised to transform capital markets. Technologists are relying on blockchains to build genuinely global marketplaces—markets that are decentralized, geographically agnostic, and accessible to all. Blockchain technology is being explored to improve the efficiency of traditional financial services, creating

---

[3] *See* The Brooklyn Project, https://thebrooklynproject.consensys.net/.
[4] *See* PRIMAVERA DEFILLIPI & AARON WRIGHT, BLOCKCHAIN & THE LAW: THE RULE OF CODE (forthcoming Harvard University Press 2018).
[5] *Ibid.*
[6] *Ibid.*

digitized financial agreements that are settled and cleared on a bilateral basis with less of a need for third party administration. Perhaps of greater long term importance, blockchains are securing scarce digital assets (often referred to as "tokens") and representations of digitized assets, which parties transfer using smart contracts in a secure and largely irreversible way, with less of a need for centralized intermediaries.[7]

Blockchain-based tokens are powering new forms of crowdfunding, often referred to as token sales, which have resulted in the sale of roughly $4 billion worth of assets last year alone. Token sales represent a potentially potent new tool for entrepreneurs to build powerful new technology platforms and hold the potential to democratize access to capital, helping to spur innovation throughout the United States.[8]

The impact of blockchain technology is spreading to the legal industry and other industries heavily reliant on contractual arrangements to structure business activity. Smart contracts are ushering in a renewed interest in "computable contracts," or contracts that can be processed and understood by machines. With blockchain technology, we soon may move beyond an era of agreements written predominantly or entirely in a natural language, replaced instead by agreements written, at least in part, in code.[9]

Outside of the private sector, governments across the globe, including China, Japan, and the European Union, are increasing experimentation with blockchain technology, exploring whether blockchains can secure and manage critical public records, including vital information, identity, and title or deeds to property, and whether blockchains can improve government procurement and taxation processes.[10] By leveraging the tamper-resistant, resilient, and non-repudiable nature of a blockchain, governments are looking to guarantee—with a high degree of probability—the integrity and authenticity of key governmental information and prevent cyber security attacks. They are also looking to streamline and automate basic government services.

Through these efforts, it is conceivable that blockchains could anchor new public digital infrastructure, and potentially even global and transnational systems, which are available to anyone with an Internet connection. Blockchains could underpin universally accessible, secure

---

[7] Jonathan Rohr and Aaron Wright, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets* (October 4, 2017), Cardozo Legal Studies Research Paper No. 527, University of Tennessee Legal Studies Research Paper No. 338, at https://ssrn.com/abstract=3048104.

[8] *Ibid.*

[9] DeFillipi & Wright, *supra* note 4.

[10] For example, the E.U. recently launched a "Blockchain Observatory and Forum," with the support of the European Parliament to "promote European actors and reinforce European engagement with multiple stakeholders involved in blockchain activities." *See* European Commission, Press Release: European Commission Launches the E.U. Blockchain Observatory, Feb. 1, 2018, http://europa.eu/rapid/press-release_IP-18-521_en.htm. China is experimenting with blockchain technology to collect taxes and issue invoices. *See* "China Will Experiment with Using Blockchain to Collect Taxes," MIT Technology Review, August 7, 2017, https://www.technologyreview.com/the-download/608570/china-will-experiment-with-using-blockchain-to-collect-taxes/. Japan is developing, in conjunction with shared ID systems for banks. *See* "Japan Developing Shared ID System For Banks," Nikkei Asia Review, Sept. 21, 2017, https://asia.nikkei.com/Tech-Science/Tech/Japan-developing-shared-ID-system-for-banks (noting that the initiative is being jointly developed by the Japanese Financial Services Agency and various financial institutions).

decentralized voting systems, transnational land and intellectual property registries, and global marketplaces available to all.

Extending beyond governmental services, blockchains are increasingly being explored to control devices and machines, with smart contracts defining the operations of Internet-connected devices. If these attempts prove successful, blockchains could foster a new era of machine-to-machine and machine-to-person interactions that could potentially change the very nature of our relationships with physical goods.[11]

Despite these opportunities, the disintermediated and transnational nature of blockchains makes the technology difficult to govern and makes it difficult to implement changes to a blockchain's underlying software protocol. Because public blockchains are pseudonymous, and because they have a tamper-resistant data structure, blockchains can be used to coordinate socially unacceptable or criminal conduct, including conduct facilitated through autonomous software programs.

Of greatest present concern, a slate of new more anonymous digital currencies, like Monero, are making it progressively easier to avoid anti-money laundering and other financial rules related to payment systems by emulating hard-to-track hand-to-hand money like cash and coins. These more anonymous digital currencies rely on advanced cryptographic techniques (such as zero-knowledge proofs and ring signatures) to obscure the origin, destination, and amount of every transaction facilitated by a blockchain. Entrepreneurs are using blockchain technology to avoid securities laws requirements, often with the aid of complicit lawyers and other advisors that emphasize form over substance. Cryptocurrency exchanges, particularly those located abroad, appear to have implemented weak measures to prevent abusive trading practices, and new decentralized marketplaces and exchanges are emerging which could operate without any centralized operator policing the network for illegal activity.

Blockchains also present a number of technological limitations. Existing blockchains are not as powerful and fast as other data management technologies and only can record a comparatively few number of transactions per day, as compared to current databases.[12] The encryption that these systems rely upon may be impacted by quantum computing.[13] And,

---

[11] DeFillipi & Wright, *supra* note 4.

[12] For instance, the Ethereum blockchain processes more transactions than any other blockchain and only processes roughly 800,000 transactions per day—far less than the trillions of messages sent across the Internet, or the 150 million daily transactions handled by credit card companies such as Visa. *See* Ethercan, "Ethereum Transaction Chart," https://etherscan.io/chart/tx (last accessed February 8, 2018). What's more, it takes approximately 15 seconds for an Ethereum transaction to be validated by the network and recorded to the shared data set, in contrast to the fraction of a second it typically takes a database to store and record information. *Id.*

[13] *See* Michael Crosby et al., *Blockchain Technology: Beyond Bitcoin*, 2 APPLIED INNOVATION 6 (2016) ("The basis of BlockChain technology relies on the very fact that it is mathematically impossible for a single party to game the system due to lack of needed compute power. But with the future advent of Quantum Computers, the cryptographic keys may be easy enough to crack within a reasonable time through a sheer brute force approach. This would bring the whole system to its knee."). Note that researchers at the Russian Quantum Center, the Steklov Mathematical Institute of Russian Academy, and the Institute for Quantum Science and Technology have proposed a possible solution to the quantum-era blockchain challenge. *See* E.O. Kiktenko et al., "Quantum Secured Blockchains," May 29, 2017, https://arxiv.org/pdf/1705.09258.pdf.

programming smart contracts has proved difficult, requiring research into formal verification and improved programming techniques.[14]

Due to the nascent nature of blockchains, and the fact that much of the innovation around blockchain technology is still occurring here, the U.S. government has the unique ability to shape the development of the technology by passing laws and regulations that will either constrain or promote the technology's growth and adoption. The United States could choose to implement regulations that make it expensive or difficult to develop or operate a blockchain-based service. Conversely, the U.S. could implement favorable regulatory frameworks to protect businesses experimenting with blockchains as part of pro-innovation policies.

Given the early stage of development, it still is possible to capture the benefits of blockchain technology, while limiting its downsides. The U.S. has the ability to rely on civil society, contractual negotiations, voluntary agreements, and ongoing marketplace experiments to solve blockchain-related regulatory problems. And, even where collective action is necessary, there are opportunities for industry self-regulation and private sector leadership.

As a guiding principle, however, it is my hope that the U.S. proceeds with thoughtful, technology-neutral regulation that:

- Permits the exchange of blockchain-based assets and scarce digital goods, particularly those used, purchased, and enjoyed by consumers;
- Enables parties to build new blockchain-based protocols, without fear of regulatory scrutiny to address the technical limitations outlined previously;
- Provides a predictable, minimalist, consistent, and simple legal environment that protects consumers without insulating entrenched market participants; and
- Re-examines existing laws and regulations that may hinder blockchain-based commerce.

To support these research and policy goals, I would encourage Congress to contemplate commissioning a National Blockchain Commission that would aim to cement America's technological standing and increase economic growth and innovation by exploring ways to invest in blockchain-based research—through prizes or otherwise—and to help ensure that blockchain-based innovation occurs here. The commission could: (i) help devise common principles to guide the federal approach for regulating blockchain technology, across a range of sectors, protecting values like financial privacy, personal autonomy, and consumer protection; and (ii) hold hearings, conduct research, and make recommendations for industry, the Executive Branch, and Congress.

Through the above approach, we can ensure that the United States remains the best place to develop, launch, and grow a blockchain-based project. The United States can maintain its lead

[14] *See* Karthikeyan Bhargavan et al., "Formal Verification of Smart Contracts," In Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, pp. 91-96. ACM, 2016 (describing the challenges of creating secure smart contracts).

when it comes to Internet-based technologies and implement sensible guardrails to guide its development.

Thank you for your time and I look forward to your questions.

Aaron Wright Short Narrative Biography

Aaron Wright is an Associate Clinical Professor of Law at the Benjamin N. Cardozo School of Law and is the Co-Director of Cardozo's Blockchain Project. Professor Wright's research focuses on blockchain technology, and in particular smart contracts, decentralized organizations, and the regulation of autonomous code-based systems. He is the co-author of the book *Blockchain & the Law: The Rule of Code* (Harvard University Press, March 2018), and is the co-founder of the smart contract-based project OpenLaw (http://www.openlaw.io), built in conjunction with ConsenSys, Inc. Professor Wright serves as the chair of the Enterprise Ethereum Alliance Legal Industry Working Group, serves an academic fellow at Coincenter, and is an editor of *Ledger*.

Professor Wright received his J.D. from the Benjamin N. Cardozo School of Law, where he served as the editor-in-chief of the Cardozo Law Review, and received a B.A. from Tufts University.

Chairman ABRAHAM. I thank the witnesses.

If I understand the blockchain technology, then it is going to be transformational. We're going to go to questions, and I'm going to recognize myself for the first five minutes.

And your testimony has helped. Being a physician that has used electronic medical records in the past and to see their advantages but certainly their disadvantages—I have got a hospital down the road six miles that I can't talk to with an EMR. This technology could certainly be eye-opening and certainly great for patient care.

As a farm guy, I do believe that national security is food security and vice versa. And, Mr. Yiannas, your testimony as to the supply chain is very eye-opening for me. You know, I consider our farmers and ranchers our thin green line, and I think that maybe our Achilles' heel in this nation as far as our national security is concerned is if we have a breach in our food security.

I took some notes during your testimony, and I'm going to just going to ask a couple of questions. Mr. Jaikaran and then Dr. Romine and Mr. Cuomo referenced that this system is tamperproof, that it's immutable, that it can still continue to operate if bad actors are in place, that there has to be a private key, that quantum computers are doing all this fancy and lightspeed stuff. But I'm still concerned. How is anything—I mean, we know what happened with Bitcoin and how it was breached. How is it tamperproof? And I'll go to you, Mr. Jaikaran, first.

Mr. JAIKARAN. Yes, thank you for the question. When we discuss the tamperproof attributes of blockchain, we're focusing on the mathematics behind it, that cryptographically we can trust that the identities that are saying they are conducting those transactions are and that those transactions are being validated by other users on the blockchain.

Additionally, once it is added to that ledger, it cannot be changed from that point forward without the other users of the blockchain knowing that it was so that someone couldn't go back in time and alter a transaction and expect that to be reported as the truth.

Chairman ABRAHAM. Well, let me interrupt you. Could there be collusion between a group of users that could change the dynamics of the program?

Mr. JAIKARAN. Yes, sir. That is one of the risks that a large group of users on the blockchain agree to conduct illegitimate transactions and they have legitimate identities, so now they are manipulating what one may want to consider to be that one truth to benefit their transactions going forward. This is significantly easier on blockchains that are new, a little bit harder on blockchains that are already established just because of the amount of data that would have to be manipulated.

Chairman ABRAHAM. So, Dr. Romine, is there any standards in place at this time that can prevent a collusion type of event from occurring or for private keys being breached in a manner where more than one could be breached?

Dr. ROMINE. Let me take those questions separately. The issue of subversion and changing of records, as Mr. Jaikaran correctly states, would require in most cases the collusion of a majority of the participants involved, and that's going to be extremely difficult.

Chairman ABRAHAM. While I can see where in a Walmart situation where you have literally millions of people involved that would be, but if you had a smaller group, I can see a potential issue there.

Dr. ROMINE. If you do have a smaller group, it is easier to do but still likely to be visible to the entire community that a fork took place and that an activity that went back in time in essence to change previous records took place. So it would be difficult to do it without detection even in that case.

Chairman ABRAHAM. And I want to get to one more question and this is to Mr. Yiannas. Are Walmart's efforts utilizing blockchain technology and supply chain and data—are very promising. I think they're on the cutting edge. With your success, do you see other industries or large corporations taking advantage of this technology?

Mr. YIANNAS. Yes. The response to our pilots have been really interesting. We've had companies from all over the world contact us with an interest in what we're doing, wanting to learn more, and actually wanting to participate, and so there's a growing body of interest certainly within the food sector. It's really, really large. We also see other industries having an interest—for example, it has implications for sustainability, it has implications for food waste, and so we think it just has applications for supply chains in general.

Chairman ABRAHAM. Okay. And I'm out of time.

Mr. Beyer, you're recognized for five minutes.

Mr. BEYER. Thank you. Thank you, Mr. Chairman. I'd like to first begin and ask unanimous consent to introduce a letter from Congressman Polis for the record, who——

Chairman ABRAHAM. Without objection.

Mr. BEYER. —co-chairs the Blockchain Technology—thank you.

Dr. Romine, you talked about immutable, distributed, resilient, so I assume that this—the blockchain will exist in clouds throughout the world and computers throughout the world?

Dr. ROMINE. That's right.

Mr. BEYER. So is the only thing that could disrupt it then is an electromagnetic pulse or——

Dr. ROMINE. That's certainly one catastrophic scenario that could jeopardize large segments, but in many cases certainly for the public blockchains are currently being used, the distribution would be difficult to track down geographically I think. It might be difficult to determine exactly where the entirety of the copies of the blockchain exist, and so finding a way to target the entire blockchain would be very, very difficult.

Mr. BEYER. Is it likely to exist in more than one place at a time then also——

Dr. ROMINE. For——

Mr. BEYER. —for a variety——

Dr. ROMINE. For public chains, absolutely. This distributed nature is one of the strengths of the resilience of blockchains.

Mr. BEYER. So as long as we have electricity, we're probably okay?

Dr. ROMINE. We probably are.

Mr. BEYER. Okay. Good. Mr. Jaikaran, the—you wrote about mining and how people—you have to create incentives and the different ways that mining can go on. It conflicts a little bit with later

testimony that there was a need for mining on it. Is there going to be a continuous need for people to be going to Iceland and spending lots of electricity and computer resources to develop the next block in the blockchain?

Mr. JAIKARAN. The use of—users mining for blockchain applies in a certain consensus model, particularly proof of work, if they have to solve a really difficult problem to show that this is a valid block in the chain. Other proofs of work may not require that proof of stake, a round-robin system where different users on the chain—it's just their turn to produce a block. These are based partially on the trust model that the users have amongst themselves apart from the blockchain, so if I'm in a business community, I already—I may already have a business relationship with other users and I may be able to use some other proof-of-work model to develop that next block. Those other models take less power and maybe even be faster to post that next block. So partly it depends on the users involved, as well as how they've developed the blockchain, what specific technologies they are choosing to use.

Mr. BEYER. So the logical next question is are blockchains infinite potentially?

Mr. JAIKARAN. I think the limitation to the blockchain would be the computational power you have to devote to it, how much storage you have, your bandwidth, your processing power.

Mr. BEYER. They get ever longer, correct?

Mr. JAIKARAN. They can continue to grow, yes.

Mr. BEYER. And does it then require evermore power to decrypt them, to read them, to——

Mr. JAIKARAN. Only—to read them, no. Once it's posted, any user on the blockchain should have access depending on the rules of the blockchain that was developed. To develop the next block, it should follow the same consensus model. If someone were on it to attack a much larger blockchain, though, that does get much more difficult.

Mr. BEYER. Okay. Dr. Romine, you mentioned that the development of quantum computing and the ability to break up these—can quantum computing be integrated into blockchain to make it ever more secure?

Dr. ROMINE. That's a fascinating question. I think one of the things that we are pursuing publicly—several months ago, we announced a competition essentially for what we call the post-quantum cryptography that is cryptographic algorithms that are secure even in the face of quantum computing and traditional computing. Once those algorithms are developed and promulgated, then yes, those algorithms would be able to replace the current public-key encryption systems that are securing the blockchain and be more secure in a quantum world.

Mr. BEYER. Okay. Very cool.

Mr. Wright, you talked about market-based or game theoretical mechanisms for reaching consensus. This is a very cool phrase but what does it mean?

Mr. WRIGHT. Yes, I think it means the way that various different parties on the network decide that there's a valid block and that they want to add it to this underlying chain link of transactions. So, for example, for proof of work, you have to run this complex

mathematical computation in order to prove that this is a valid block and it gets added to the chain, but you also have to pay fees that are related to it, so it's this dynamic between the mechanism with which you add information to the blockchain along with the fees that are charged by members particularly on public blockchains.

Mr. BEYER. So they're not really reaching consensus on areas of disagreement; they're reaching consensus on the fact that this given block is valid——

Mr. WRIGHT. Exactly.

Mr. BEYER. —or true or——

Mr. WRIGHT. That it follows the protocol.

Mr. BEYER. Okay. My time is up, but thank you very much.

Chairman ABRAHAM. Thank you. Great questions.

Mrs. Comstock, five minutes.

Mrs. COMSTOCK. Thank you, Mr. Chairman. Really this has really been a fascinating hearing and topic, and thank you for holding this hearing.

I was meeting with some folks last week on this about the caucus, so they did highlight they needed more diversity in the caucus, so I do plan on joining it. And thank you for highlighting the caucus, too.

In my opening statement I referenced the Office of Personnel Management data breach and, you know, the OPM notifying us, and I was wondering if you could go into some more detail on how we could use that technology to better protect personal and sensitive data stored by the government? Sure.

Mr. CUOMO. So, Chairwoman Comstock, we are working with companies, as I referenced. One is SecureKey in Canada, and I think that's probably the furthest along to proving out digital identity blockchain, as well as working with the Sovrin Foundation, who's working on digital identity protocol standards on blockchain.

In the case in Canada, they've gathered an ecosystem of all the major banks, Province of Ontario, British Columbia, and others to form a digital rights management system is probably the best way I can word it where citizens are the rightful owners of their data, and they basically in a very simple interface that's not much more complicated than your Facebook app give permission—for example, if I go to a real estate company to rent an apartment, I'll give my bank and my DMV permission to answer any of the questions, almost like it's a music license. I'm giving them license to answer my question and vice versa. I'm giving the folks answering the question the right to answer the question.

And there are stipulations even in NIST talking about avoiding honeypots of data, and I think a lot of the major security breaches—it's a good idea not to put all your eggs in one basket. And one of the misnomers about using blockchain for identity is that you actually put personal identity information on the ledger. You don't. You put proofs of permission. You put the digital rights on it. And, you know, it becomes almost a routing system for how you can have people interact with accountability on your identity information and making it far less visible.

And last but not least, it's much harder to track your identity and usage, so there's stipulations about these things called triple

blind data exchange where the requester doesn't know who the provider is, the provider doesn't know who the requester is, and the network provider doesn't know either. And that makes it, again, very thorough to know so that only the parties who need to know actually get to know.

Mrs. COMSTOCK. Okay. Dr. Romine?

Dr. ROMINE. Yes, from my perspective I think the important issue here is that, as Mr. Cuomo mentioned, storing PII in the blockchain itself is not recommended. This is not something that you want to do. In the example that Mr. Jaikaran used for access to medical records points that out. The medical records themselves still are retained on the private servers of the medical provider, but access management, access control, and auditability of access is provided through blockchain. So there are opportunities here to do some really interesting things in this space.

Mrs. COMSTOCK. Okay. Mr. Jaikaran?

Mr. JAIKARAN. Yes, ma'am. What may be particularly interesting is not the use of blockchain technology itself to protect sensitive data but some of the technologies that underpin blockchain, so public-private key encryption, hashing, and particularly loggings, that we know when data is being used, we know who is accessing that data, and we know when access—when data is being changed. Those technologies, particularly for very sensitive information that's not published to the blockchain, can certainly help protect data that we have today.

Mrs. COMSTOCK. Thank you. I yield back, Mr. Chairman.

Chairman ABRAHAM. Thank you, Mrs. Comstock.

Mr. Lipinski, five minutes, sir.

Mr. LIPINSKI. Thank you, Mr. Chairman.

There's so much to really cover here and talk about and try to understand, but I think I want to get down to sort of whatever we can do in five minutes, get down to the question for us here. Is Congress doing enough to foster a coherent strategy regarding, you know, blockchain research and development and a unified regulatory strategy where appropriate government guidelines on dealing with blockchain-based technologies? So I know we can't cover that in five minutes, but let me start with Professor Wright because I know you've suggested that Congress initiate a National Blockchain Commission to address some of these issues. Can you just briefly expand a little bit on that? And then I want to get some reaction to what you have to say.

Mr. WRIGHT. Sure. So the idea with the blockchain commission would be to provide a degree of uniformity and a unified approach with regard to various different regulatory challenges that have emerged with regard to blockchain technology. You know, just from the statements from——

Mr. LIPINSKI. Unifying across the government or——

Mr. WRIGHT. Right, across the federal government.

Mr. LIPINSKI. Across—okay.

Mr. WRIGHT. So, you know, just some issues just raised by the witnesses' testimony today, there's privacy issues, identity management issues, key management issues, consumer protection. There's issues related to securities laws, commodities laws, and also issues related to the use of blockchain technology for currencies. And

there's competing interpretations that have been issued already by various different federal agencies, so the thought would be to explore if we can have a common and unified guiding principles in order to ensure that the technology can develop in a mature way.

We did this in part with the internet where we just distilled down a couple guiding principles and, in part some have commented that this is one of the reasons why so much internet-related innovation occurred here. I think it could be an opportunity again to look back to what we did when it came to internet policy back in the mid-1990s and apply that same idea to blockchain technology.

And in addition, the other witnesses mentioned a number of different technological issues related to it, and a number of members in the private sector are trying to solve those issues, but any government support to address issues like scalability, issues related to developing quantum-resilient blockchains, issues related to other technical limitations that are currently present with blockchains would be helpful and I think encouraged.

Mr. LIPINSKI. And I ask our other witnesses: Do you generally agree with that or is there anything that you would disagree with in terms of what the federal government should be doing? Mr. Jaikaran?

Mr. JAIKARAN. Sir, so what we see the federal government doing today is a variety of activities under the authority of that agency. So Mr. Romine talked about the NIST blockchain workshop, which is developing some use cases. We see that the Government Services Administration, GSA, is hosting other federal agencies to talk about potential applications of blockchain for government uses. Also, the Department of Homeland Security is issuing grants to try to overcome some of the issues surrounding blockchain to private industry to come up with solutions.

Where we see this today is still in this testbed, trying to develop an understanding of technology, develop an understanding of how it can be applied, and then trying to develop a consensus amongst these tests. We have not yet seen a common federal "this is our path forward."

Mr. LIPINSKI. Mr. Cuomo?

Mr. CUOMO. Yes. And I would also like to reiterate that there is some really good work being done by the Congressional Blockchain Caucus, right, and that's Representatives Polis and Schweikert. And we've had already one workshop around digital identity and had some really good outcomes. Next week, we have one on payments and one to follow later with on supply chain. And particularly, what that's doing—in introducing members from NIST, IBM was really informed by what the government was doing and actually helped us on policy and interactions working with our clients like with SecureKey in Canada, as well as that's where we met members from the Sovrin Foundation that really turned us on to some of the emerging standards. So those types of interactions are paying off by bringing government agencies and industry players together, so I want to encourage that.

Mr. LIPINSKI. Mr. Yiannas?

Mr. YIANNAS. The only thing I wanted to add, I don't have specific advice, but just conceptually, you heard that we're scaling,

testing, and learning together, so there's a lot of learning that's going on. And a lot of this is happening in the private sector. There's collaboration happening with a lot of private entities. The notion that maybe the public sector could participate in some of these tests I think would be very beneficial. One of the things we like to say is that blockchain truly democratizes the benefits. Everybody benefits. So if you think of the food examples I gave, not only will suppliers benefit but regulators will, too, being able to conduct tracebacks. Consumers will. And so I would just recommend that they get involved in some—pick out the right agency to get involved in some of these pilots that are testing, scaling, and learning together.

Mr. LIPINSKI. Thank you. I'm out of time. I'll yield back.

Chairman ABRAHAM. Thank you. A fellow Louisianan, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman. I thank the witnesses today. This is fascinating testimony.

We certainly recognize the tremendous promise of blockchain technology and supply chains and—throughout the private sector. I also recognize the great threat, potential threat in the government sector. I think we need to move forward very cautiously as we explore the broadened use of blockchain technology.

The precise tracking of valuable items and inventory at the Walmart level is great. Everyone is within that sphere. There's a financial benefit for everyone involved within the blockchain. But to expand that technology into the government sector, you're dealing with bad actors across the world that could perhaps infiltrate that blockchain—this occurs to me—and know precisely because of the accuracy—because of the very accuracy that you referred to, sir, in the Walmart example for tracking the mango slices in 2.2 seconds versus 7 days, that same technology would allow a bad actor tracking government-secured inventories like weapons or uranium, et cetera, to the exact location.

So I'm concerned about the verification. Mr. Jaikaran, you referred to authorized entities. How do we—how would we know—explained to us—help us grasp how the digital or virtual identity versus actual identity of a blockchain user is verified. How do we know that a bad actor does not have possession of a private key? How do we know a private key has been stolen until the damage is done—been done?

Mr. JAIKARAN. Thank you, sir. As Mr. Romine has discussed earlier, many of the cases that we hear of Bitcoin being stolen is because a private key has been taken and used, so in many examples we've seen to date, we do not know if a private key has been stolen and used. We find out about the transaction after it has posted.

For some of the more sensitive supply-chain concerns, the implementations of blockchain that may be used for that are permissioned and private, meaning that not anyone can join that blockchain and not every person on that blockchain will have access to all the rights on that blockchain. So there's a level of control that then governs who has access to the data, who can publish the data, and who then can transact that data.

Mr. HIGGINS. That's very promising, I believe, for the private sector and potentially for the government sector. I see a public-private

partnership emerging as this technology emerges. I'm concerned about quantum computing.

Dr. Romine, you referred to in your submitted testimony a public key and a private key. They're mathematically related to each other and that the Federal Information Systems Processing Standards specifies elliptic curve digital signature algorithms, which is a common algorithm for digital signing using blockchain technologies, and yet we're concerned about protecting that algorithm from quantum computing. And you referred to—that NIST is leading the global effort to ensure that this—that encryption is available to industry prior to the emergence of quantum computing, but how would we know that quantum computing has emerged until we have observed its interaction with blockchain technologies?

Dr. ROMINE. That's a very good question, Congressman. I think the issue here is there's a general recognition that there's a lot of investment around the world in the attempt to develop quantum computing. I think the general consensus here is that it is still a significant number of years away from maturity until we reach what we call a cryptographically relevant computer—quantum computer. The day that that happens, I agree with you; I doubt that there's going to be—at least potentially there may not be a headline around the world that says we've now crossed from a non-quantum computer state into a quantum computer state. It may be that some of the people developing that technology would like to use it before it becomes public. But our goal is to try to move with alacrity in the development of quantum-resistant cryptography so that we are ready in the event that that day occurs.

Mr. HIGGINS. You stated a number of years. Can you give us an idea of a window, sir?

Dr. ROMINE. The estimates vary. Publicly available estimates vary anywhere from 15 to 30 years. I don't really know. It could be shorter than that if there are dramatic improvements in technological advance that we can't really predict right now.

Mr. HIGGINS. I thank you for that answer, sir, and thank you all for testifying today.

Chairman ABRAHAM. Thank you, Mr. Higgins.

Mr. McNerney, five minutes.

Mr. MCNERNEY. Well, I thank the Chairman for holding the hearing and I thank the witnesses.

Back to the present, Mr. Jaikaran, in your testimony you raise the issue of how an attacker has the ability to compromise a user's private encryption keys. Have there been any instances of blockchain compromising?

Mr. JAIKARAN. Yes, sir. When you hear cases of someone stealing Bitcoin or other cryptocurrencies, what likely happens is that that user's computer that hosted that private key was compromised or that private key was somehow taken from that user so that they could—the bad guy could perform a transaction transferring that digital asset to themselves.

Mr. MCNERNEY. So it's a matter of data hygiene. Is there some way to protect yourself from those kind of losses?

Mr. JAIKARAN. The risk here is similar to any kind of data loss. You want to ensure that you are—your machine or the network

that you're hosting that information on has proper security measures in place.

Mr. MCNERNEY. Well, thank you.

Mr. Romine, could you give us an update on the—on developing blockchain technology standards and having those standards adopted by industry?

Dr. ROMINE. Sure. The first effort that we did was to publish a general guideline to blockchain that I alluded to my testimony. That isn't so much a standards development activity as it is a means of providing a common vocabulary for people to use when they talk about blockchain. Our engagement, as you know in the United States, in general, standards development occurs in the private sector.

We at NIST—as the nation's standards organization for the federal government, we participate vigorously in many of those activities, and the ones that we're participating in now include work that's going on with the International Organization for standardization and the insights committee that we use in that effort, OASIS, IEEE the Institute of Electrical and Electronics Engineers, our ANSI colleagues, and others as well. So we're participating in technical committees and subcommittees in the blockchain arena today.

Mr. MCNERNEY. Well, I know that Walmart's developing standards for its own use. Is there any chance that those standards would be—because Walmart is a big organization, their standards would be adopted, you know, over a broad range of applications before standards have been accepted in the government?

Dr. ROMINE. Certainly, one of the things that can happen is, as de facto standards emerge or a substantial part of the private sector begins to adopt a specific standard, those standards can ultimately be brought to these standards bodies and either adopted or modified as needed.

Mr. MCNERNEY. Sir, thank you.

Mr. Cuomo, in your testimony you noted that there are currently trusted digital identity projects underway in Canada. Could you give us a little more about those projects? Are they government-led, and exactly what do they entail?

Mr. CUOMO. So in Canada there's a company called SecureKey that we're working with, and they're a small company that offered a service for citizens to use any of their bank IDs, user IDs and passwords to log into government services like motor vehicle, you know, taxation department, et cetera, so eliminating propagation of user ID and password. However, based on further examination, they thought they can do better, and with encouragement from all parties involved decided to try blockchain, and not just any blockchain but I mentioned in my testimony a new breed of blockchain, which is what we call a permission blockchain, which brings accountability and ability to surface and surf through regulations and be able to adhere to existing regulations.

So we worked with them, the banks and the government agencies, to implement a system called to VerifyMe. It was the mobile application that I mentioned before. It is about to go into pilot right now. Banks are building applications on it for increasing the efficiency of onboarding clients while doing their KYC and AML proc-

esses and streamlining those. And in general, giving citizens back the rightful control of their identity but also using established companies and institutions to kind of be their friends like in Facebook when you would friend someone. So you can turn to any of the existing relationships you have like with your DMV and you can allow them to attest to your identity, right?

So this is underway. We are about to enter pilot into that system. There are companies in the United States to—looking at that as well. It's been heavily influenced by many of the standards that my friend to the right of me have helped bring forward around data privacy.

Mr. MCNERNEY. Thank you. I yield back.

Chairman ABRAHAM. Thank you, Mr. McNerney.

Mr. Banks.

Mr. BANKS. Thank you, Mr. Chairman.

I think what is most incredible to me is how much of this is developed without overregulation from the federal government. And I guess I would direct my questions to Mr. Cuomo and Mr. Yiannas. What are you most—from a—more of a broader perspective, what are you most concerned about? Where can the government really screw this up, the continued development of this technology? Mr. Yiannas?

Mr. YIANNAS. My initial impressions of that question is maybe becoming overly prescriptive. There's a lot of innovation that's happening right now, and I think we ought to let the innovation play out. As I mentioned, I think there's opportunities for the public and private sector to do this testing and scaling and learning together, but if we start getting too prescriptive early, I think we'll stifle innovation.

Mr. BANKS. Have you seen specific examples?

Mr. YIANNAS. I have not seen any examples of that. In fact, in contrast what we've heard is from some of our federal partners, CDC, FDA, with an interest in what we're doing and learning how they might play a role or benefit, so I haven't experienced that in the area of food.

Mr. BANKS. Mr. Cuomo?

Mr. CUOMO. I'd further add to that that, as I mentioned, there is a new form of blockchain that is more suitable for business and government applications around permission blockchain versus with Bitcoin where you have open networks that are self-governed. With a permission blockchain, while the networks could be open, they are governed by steering committee members, right? So it's—again, I think it's more controlled. It's working in a more controlled environment.

So again, distancing any regulations and policy that are being levied against, you know, currency-oriented blockchain to this new breed I think is important to keep that separation because there's an immense amount of innovation that can and will happen beyond cryptocurrency, so we really want to encourage the look at that, A.

And B, there are many governments who are indulging in I would say less risky blockchain projects whether it's digital driver's license, land registry, things of that nature. So you got to be in it to win it, and I think trying out some low-risk projects, learning

from those, and participating more I would say with more tempo once you get those under your belt is what we'd recommend.

Mr. BANKS. So both of you would agree I think what this hearing is all about, that we've benefited from the development of this technology without government overreach, without regulation, and you in the private sector especially seeing the benefit of that. Both of you would agree with that?

Mr. YIANNAS. I would agree with that.

Mr. CUOMO. Yes, sir.

Mr. BANKS. Okay. Thank you. I yield back.

Chairman ABRAHAM. Thank you.

Mr. Perlmutter, you have five minutes.

Mr. PERLMUTTER. Thank you.

And to the panelists, this is great. You're—Mr. Yiannas, I want to start with you. Your little example which isn't so little of 7 days to 2.2 seconds on your supply chain on the mangoes, just the possibilities for government but other industries are tremendous, so I was just thinking about in Colorado. So we've had a lot of oil and gas development. Now we've got real estate, suburban—the suburbs growing into what were old oil and gas fields, and we're not quite sure where all the pipes are.

Mining, you know, what's coming out of the mine, to be able to go back from an environmental standard or from a real estate standard and track this in a—you know, such an expeditious manner——

Mr. YIANNAS. Right.

Mr. PERLMUTTER. —is so—what other industries are you guys working with besides the food industry? I know that's your specialty, but are there other parts, other industries in your collaboration——

Mr. YIANNAS. Yes——

Mr. PERLMUTTER. —or your consortium?

Mr. YIANNAS. In our consortium there is not. This is a food consortium. But let me just real briefly if I could say the difference between 7 days and 2.2 seconds, it's a big difference. On the one hand—not just speed. On the one hand, imagine if you just put all of the mangoes—if there were—you know, associated with an event because you don't know the source, that's 7 days of lost sales, 7 days of food waste, 7 days of small farmers' livelihoods being destroyed. You eventually say, oops, your mangoes weren't affected. On the other hand, if you don't pull them, that's a lot of potential illnesses, hospitalizations, even deaths.

But we know that there are other areas of interest within Walmart and outside of Walmart. We see interest in the pharmaceutical industry obviously, anything that's supply-chain related. We see interest in sustainability sectors. You know, how can we manage supply chains so that they're more sustainable, health and wellness so, you know, I think it's endless the people that——

Mr. PERLMUTTER. I really—the possibilities are endless here, and that's what's so exciting about this.

Dr. Romine, I want to thank you and NIST for being engaged in this and for—you know, it's a frontier. It's the Wild West in some respects, which is great. And to ultimately have some standards which kind of rein in the Wild West nature of it a little bit.

I'm kind of coming where Mr. Higgins was coming from, though. I serve on another committee which is Terrorism and Illicit Finance, and, you know, I—maybe I've watched too many Mission Impossible's, but when I hear words tamperproof, immutable, can't be hacked, I'm thinking, you know, Tom Cruise is out there someplace, and he's coming up with a way to do it.

So talk to us a little bit more about this—the quantum computing element of this. And Mr.—I'm sorry—Jaikaran—you know, for both of you because, you know, that's something I need to understand because we deal with a lot of hacking and cybersecurity issues in my other committee.

Dr. ROMINE. So I'll start just by saying the backbone of everything that we're talking about here is cryptography, and NIST has been involved in cryptographic standards for more than 45 years. It's the backbone of our cybersecurity program and something about which we are fiercely proud, the track record that we have there.

The idea that we would sit back and wait for the advent of quantum computing to render our public-key infrastructure impotent is something we can't live with, and so some years ago we initiated, and much more recently announced, the competition that I alluded to for quantum resistance so that we will be prepared in the event that quantum computing does render our current cryptosystems ineffective. Long before that happens, we will have replacements available so that we can continue to use cryptography to underpin a trustworthy information technology environment.

Mr. JAIKARAN. Thank you for the question, sir. So when we talk about the data on a blockchain being immutable and auditable, we're really saying that we trust the math, not necessarily the data that a user entered. So in a supply chain example——

Mr. PERLMUTTER. But information's required to——

Mr. JAIKARAN. Information is required to input, but it's that cryptography that we trust, that we say, ah, yes, this must be valid. There are pitfalls there, so I discussed earlier a user collusion. You could have a user physically tamper with a tracker in the supply chain and other users agree that that's going to be tampered so that what appears in the record appears to be true but it is actually somehow altered, and that might inhibit our ability to track it going forward.

With quantum, I talked about business, legal, and technology that would be applied. If you're using weak crypto as one of the specific technologies that's being applied, that can be overcome by high-performance computing or quantum computing, and that's one of the risks that those choosing to implement blockchain or any technology really must consider before they move forward.

Mr. PERLMUTTER. Well, I want to thank you all. I've got a million questions about cryptocurrencies, but this is really an outstanding panel. Thank you.

Chairman ABRAHAM. Thank you, Mr. Perlmutter.

Ms. Bonamici, five minutes, please.

Ms. BONAMICI. Thank you very much, Mr. Chairman. This is a fascinating discussion, and I really appreciate all the witnesses who are here today. I know that this technology and its applications are clearly evolving very rapidly, and I appreciate the oppor-

tunity to learn more and to hear from you and some of the—about some of the opportunities and the challenges.

I'm curious about a couple of things, first of all, the potential applications of blockchain technology in voting systems. Could any of you—maybe Professor Wright and Mr.—is it Jaikaran? Am I close? Could you elaborate on how a blockchain might play a role in making our elections more secure and trustworthy? I had the opportunity a couple of years ago to visit Estonia with the then-Chairman of the Education Committee Chairman Kline, and we had some interesting conversations about what they're—you know, what can we learn from Estonia because they have of course e-voting, i-Voting. They've done some pilots even with shareholder voting. So what are the potentials there and how could blockchain make our elections more secure and trustworthy? Mr. Wright?

Mr. WRIGHT. Thank you very much for the question. So the idea here is blockchains can store many different types of data, including potentially data related to voting. And there's been a significant amount of research over the past couple years thinking about whether or not blockchains can actually be used as a way to improve voting in a couple different capacities. For public voting systems the anonymity that's probably required for these systems to operate is not there yet, but at least for votes and voting mechanisms where the parties do not need to be anonymous, there's been some strides that have been made from researchers.

So, for example, the thought would be in the corporate setting where shareholders don't necessarily need to keep their identity anonymous, they can record their votes on a blockchain, and then you can use more of these autonomous processes called smart contracts in order to just tally them up automatically so you have an auditable trail of all the votes, and then you can use additional logic in order to improve the efficiencies of these voting processes. So——

Ms. BONAMICI. I don't mean to interrupt, but with regard to anonymity, a significant portion of the population and Estonia does vote by i-Voting, and it is anonymous, so does anybody know how they do that then if you're concerned about anonymity?

Mr. JAIKARAN. Ma'am, so one way of implementing a blockchain—remember, this is just a ledger of transactions—it's to not record the vote itself but record the identity of a voter having taken that action. So you could use the public-private key encryption to say this person, this identity has voted today at this place, but then the vote itself is not stored on the blockchain at all. The vote itself is held in some other secure system. So the voter voting is registered in the same way we would in a poll book, but the vote of that voter is still anonymous.

Ms. BONAMICI. Thank you, fascinating. Can you talk a little bit about what we are—how we in the United States compare both in terms of—and I appreciate the work of NIST. I know you're still open for public comment on your report. But how do we compare with other countries in our advancements in this field and in developing a workforce that is—will be required to work in blockchain technologies? Dr. Romine?

Dr. ROMINE. I don't have specifics about other countries' activities with respect to blockchain specifically. We do know that there's

a lot of activity in the area of cryptography around the world, and we are a leader in the United States. We're a leader in cryptography as a result of the activities of at least in part my organization. I'm very proud of that.

As I alluded to in my testimony, we're leading the world in the development of quantum-resistant cryptography as a result of this global competition that we've launched, and we've gotten a lot of interest and participation around the world.

Ms. BONAMICI. And can I ask before my time expires, could you talk a little bit about the possibility of—with the testbeds that are available with NIST, the possibility of the federal government hosting other testbeds and the ability for other researchers to use those testbeds, federally funded researchers?

Dr. ROMINE. Sure. We are not really operating so much as a user facility in this particular case, but we're always happy to talk to anyone about collaboration with us. If there are people who are interested in working with us on the development of mechanisms for testing out blockchain technologies, we're happy to discuss that with anyone who would like to reach out to us.

Ms. BONAMICI. Thank you. And as I yield back, I want to thank Mr. Cuomo for inventing the someone-is-typing indicator, which I find very useful. Thank you, Mr. Chairman, and I yield back.

Chairman ABRAHAM. Thank you.

Dr. Marshall, five minutes.

Mr. MARSHALL. Yes, thank you, Chairman.

I'll start with Mr. Yiannas.

Mr. Yiannas, I represent an agriculture district, and one of the big advantages that Kansas farmers, American farmers have—well, actually, there's several. One is their ingenuity and their hard work. Number two is our infrastructure allows us to get our goods to market as efficient as anybody, but the third thing is I think we have an incredible food safety and quality that would compete with anybody in the world, so we're excited to hear how you're using this technology.

And I think it would even give our farmers an even bigger advantage if you knew that we had consistent better quality. So as you're making this transition to this, how do you see—is, you know, food quality going to influence the purchase where Walmart's going to be purchasing its goods from?

Mr. YIANNAS. Well, it's just allowing us to be much more informed where the product's coming from and how it's being produced and how it flows. The benefits could be from increased assurances that the product's been produced safely, authenticity, the ability to track and trace products. It's the anonymity that often——

Mr. MARSHALL. Exactly.

Mr. YIANNAS. —allow some people to do unscrupulous behaviors in the supply chain with things such as economically motivated adulteration. But we've talked to farmers, and in terms of the stakeholder groups in the food system, farmers are probably one of the most important stakeholder groups that we want to hear from. And the initial read that we're getting is very positive. Farmers, when there is a food scare, are often falsely incriminated, and their crops——

Mr. MARSHALL. Exactly.

Mr. YIANNAS. —are damaged, and so——

Mr. MARSHALL. Collateral damage.

Mr. YIANNAS. —this allows them to clear their good name faster. Farmers take a lot of pride in how they produce products. It gives them the ability potentially to have a voice or a face with the customer, and so we are going to try to design a solution that's very sensitive to the farmers' needs.

Mr. MARSHALL. Anybody else want to comment on food safety? Mr. Cuomo, go ahead.

Mr. CUOMO. Yes, one of the things that I think is important is the convergence of technologies. Blockchain is certainly, you know, I think a—you know, a transformative technology but there are other I would say cousins out there like Internet of Things and AI. And especially in like supply chain taking the physical good and digitizing it on an immutable ledger I think is really important.

In my written testimony I talk about some research that IBM is doing in a snap-on to an iPhone camera lens that does a spectral analysis so, for example, if you take a picture of a vial of oil coming out of a Shell Oil plant at the origin of the plant versus the—at the pump, let's say, you can actually see the digital fingerprint as it was originally at the factory versus what you're seeing, and maybe you might find out that it has been watered down a little bit.

So you can imagine physically digitizing an important complementary technology to blockchain that—and similar to AI, you know, we're doing things with our Watson technology, for example, in diamond provenance with a company called Everledger to interpret and ingest the obligations of a very thick piece of regulation called the Kimberley Act, which is here to protect us all around proper processes around diamond mining. And what they're doing is is they're using a smart contract to ensure that the diamond certificates all follow the rules of the Kimberley Act. So these cousins I think are also very important to supply chain. They can work very well together.

Mr. MARSHALL. And we're excited to see the continued advancements in AI that you're having without us regulating you, overregulating that process. Yes, we're excited about that.

I want to turn to health records. I'm a physician as well, and one of my biggest struggles as we went through meaningful use for the hospital as well as physician practices is I explained it like this. I felt like the hospital had a Chevy. I had a Ford. The doctor, the orthopods across town had a Cadillac, and they wouldn't talk to each other or maybe one was in Spanish and one was in French and one was Greek or something. How do you all see this—solving that dilemma where maybe—I would love to hear more about the patients having control of their own records. Is it going to help solve this problem where we have 10, 20 different computer systems out there that speak different languages? I'm not sure who's our health care specialist. Go ahead.

Mr. JAIKARAN. Thank you for the question. In this example, the—and I speak about it in my testimony as well—providers maintain that health record in a manner that is consistent with federal and state law——

Mr. MARSHALL. Sure.

Mr. JAIKARAN. —so there's still a variety of systems in use. What the blockchain may publish is permission to that record. So rather than a patient having to drive across town to pick up a disc of that health records to take over to their next provider, providers could see that a permission for access to that record has been published to this blockchain, and then providers can then talk amongst themselves to transfer that record.

This still comes with some pitfalls. One, all the providers have to be on the same blockchain so they all have some kind of identity, a public and private key, and users have to take a more active role in managing that record for themselves.

Mr. MARSHALL. But do you think this solves—right now, what's happening in doctor's offices, I literally have to send it to them, they print it and copy it, and then they paste it into the record. You think this will solve that problem?

Mr. JAIKARAN. It is a potential technology that can be applied to that problem. Whether or not it solves it, it depends to be seen on specific application.

Mr. MARSHALL. Okay. Thank you. Mr. Chairman, I yield back.

Chairman ABRAHAM. I thank you, Dr. Marshall.

Ms. Esty?

Ms. ESTY. Thank you, Mr. Chairman. And my apologies. This is one of those multi-hearing days and meeting days. But I did appreciate that question on health records because I just came from a meeting with Secretary Shulkin at the VA, and one of the topics we were discussing is exactly how do we deal with medical records and do we have a better way of dealing with that. So I'll be interested to follow up.

Blockchain technology has the potential to make game-changing transformations to our digital economy and financial security. We're seeing countries like China and Switzerland, who are front and center in developing an innovative hub for blockchain technology. Switzerland, known as Crypto Valley, is home to an institution that targets the development of blockchain and virtual currency startups. Last year, China launched the Trusted Blockchain Open Lab to support the application of blockchain technology across various sectors.

Mr. Wright, in your testimony you recommended to Congress to establish a National Blockchain Commission in order to drive blockchain innovation through prizes or otherwise in the United States. Can you point to current innovative hubs or economies that favor blockchain development, and what are the characteristic that makes those hubs favorable to blockchain development, and how could a national commission replicate those best practices?

Mr. WRIGHT. Thank you very much for the question. So the innovation hubs are fortunately still in the United States, so there's a tremendous amount of activity in New York. There's a tremendous amount of activity obviously in the bay area. And that's really being driven by the private sector. So I do think that we're actually on great ground when it comes to the innovation occurring here, but I do think that there's a number of technical and legal limitations that could either enhance or inhibit the technology going forward. And the idea would be to pinpoint areas where we need to

shore up and provide additional research, so one area that hasn't been addressed yet is for these autonomous computer processes known as smart contracts. They have a number of different bugs and different problems emerging with them. It would be great to provide research for formal verification so that we can understand this new computing paradigm, issues related to quantum computing, et cetera. I think if we can provide that research, we can ensure that the private sector then can take the learnings from that research and bring it to the public.

Ms. ESTY. And who do you think is best positioned to be conducting that? Where do you see—who do you see as overseeing that? Obviously, there's an enormous demand for talent and we don't have the talent pool to fill all those demands, so we're going to be having to compete with other—with agencies that are already trying to recruit these same researchers from this same talent pool.

Mr. WRIGHT. Yes, I think that's a great question. And, you know, blockchain technology—and some have analogized it to being as impactful if not more impactful than the internet, so it hits a number of different industries, it hits a number of different sectors, so I think if we were to take this approach, it would require multiple stakeholders to become involved, to think about it. Academia obviously could play a huge role here as well through grants or other ways to fund innovation.

Ms. ESTY. I mean, you mentioned prizes. Do you see this as grants or prizes? Obviously, there's—again, you may have noticed our budgets are a little tight here. The research budgets in the President's proposal are being cut across many different agencies. There are very few they're getting plussed up, VA and Defense Department about the only ones. Does that suggest it ought to be in DARPA? I mean, where do we actually—where would we park such an initiative practically? Who's got the expertise and where do we think they would be best positioned to move forward?

Mr. WRIGHT. So with regard to prizes, that was mentioned because it actually complements what's organically happening in the private sector. A number of different projects that are examining and exploring blockchain technology in the private sector have already implemented bounty programs or different ways to try to solve some of the technical issues. So I think the government would complement what's already emerging in the private sector.

With regard to where it's housed, I would defer to the wisdom of these subcommittees in order to determine that appropriately.

Ms. ESTY. Anyone else want to weigh in on that? Yes, Mr. Cuomo.

Mr. CUOMO. Yes, just reflecting on one of the recommendations, which was to thoughtfully insert blockchain into projects already funded, and I think there's good funding going on today and we can leverage that. And I pointed out in my testimony the Small Business Innovation Research program I think, so I think tacking onto and encouraging within the context of already funded I think is a great idea, as well as the National Blockchain Commission.

Ms. ESTY. Anyone else with other thoughts? Yes.

Mr. JAIKARAN. Something Congress may want to consider when thinking about where to park blockchain is to divide a blockchain for its intended use. Are you interested in supply chain manage-

ment for food safety? That might lend itself to one agency versus the international shipping of blockchain and something coming into our ports. That may make it appropriate for another agency. So rather than look at the technology itself, the application of the agency and the expertise of that agency may drive where that particular implementation would reside.

Ms. ESTY. Thank you. I appreciate—although I will note with that the shortage of the workforce makes that hard to do because then you're going to have to have that capacity in lots of different agencies, and frankly, right now, with our efforts to support a STEM workforce, we know we don't have what we need right now and we've got cybersecurity issues, defense as well as offense, that we're also trying to recruit for, so that is aspirational but perhaps not realistic right now to be able to park this in each of the agencies, although I think it does make a great deal of sense.

Thank you and I yield back.

Chairman ABRAHAM. Dr. Foster.

Mr. FOSTER. Thank you, Mr. Chairman. I appreciate the ability—my ability to sit in on this committee. So now actually you've had the opportunity to be questioned not only by the only Ph.D. mathematician but also the only Ph.D. physicist in the U.S. Congress, so I won't go too deeply into the nuts and bolts of quantum computing in the interest of time, but I guess my question is probably mostly for Mr. Wright.

Digital contracts seem like they're really an area where this could be transformative. And it seems to me there are two classes of these, one where you need a governing body that can break the contracts under some circumstances and one where you're comfortable just letting, you know, the digital process play out. And I was wondering if you've thought about, you know, the classes of problems that can be solved by those two.

Mr. WRIGHT. Sure. So thank you for the question. One of the emerging-use cases for blockchain technology is to memorialize parts of legal agreements in code, in software, so instead of having a natural language agreement, you would have all or portions of that agreement memorialized in some sort of software-based system. Smart contracts are unique, particularly on public blockchains and their ability to run autonomously across a number of different computers at the same time, so that means you could potentially preclude them from terminating at some point in time. But at the same time they're software, so you can program them in different ways, including ways to halt or terminate them.

The real fundamental value for these smart contracts when it comes to legal arrangements is that blockchains have proven at least in the public setting to be pretty exemplary and exceptional in securing digital assets of different various stripes, including virtual currencies and representations of physical and/or other digital assets, and you can use these programs to seamlessly transfer them.

So, for example, in the project that I mentioned that I'm working on called OpenLaw, we were able to model out an employee offer letter, and the employee offer letter, instead of it—it articulated a payment schedule, and instead of getting paid every two weeks. you could get paid every minute, right? And we can plug into that

a smart contract that could actually remit tax payments automatically, assuming that the government was willing to accept tax payments and virtual currency. And that obviously is a proof of concept but I think it points to a future where our commercial relationships are much more dynamic and it is a—represents a really new frontier for how we think about commercial arrangements.

Mr. FOSTER. And yet if you found that the employee made fraudulent presentations in their application for the job, you need something like a court that has to go back and be able to digitally break this digital contract so the payments don't happen.

Mr. WRIGHT. Yes, absolutely. So I think the consensus is emerging that we will have agreements that are written in natural language that only reference these smart contract programs, and of course courts would be able to administer them if there's a dispute. And on top of that there will be technical safeguards that would be put in place so that the parties could terminate the performance obligation during the course of performance.

Mr. FOSTER. Okay. So these sound like quite complex things even to accomplish something simple.

Mr. WRIGHT. Yes. I think they're complex but over time they should simplify and then could have a broad range of impact.

Mr. FOSTER. Yes, or perhaps standardized, remain complex but have the standardized boilerplate and the small amount of customized—but it's fascinating.

There are a couple of near-term things. Land registries using blockchain are being pursued by a handful of countries that I'm familiar with. And the other—and several countries are talking about issuing fiat currencies, so these are not like, you know, Bitcoin where it just floats and has no intrinsic value. This would be something where the government treasury would guarantee to accept them for payment of taxes or give you a real cash dollar back and so that they wouldn't—you know, they'd be solid. And I was wondering what your—what are the near-term status of either of those whoever is most familiar with land registry efforts, for example? Mr. Wright?

Mr. WRIGHT. This is a great question. So the idea here again is to record information related to title to property or deeds to property on a blockchain. In the United States obviously the land title recordation system is quite fractured, so it would require a lot of coordination between various different state- and county-level officials in order to build these types of systems. But that's the promise. The promise is we can begin to record evidence of ownership on a blockchain and potentially develop a set of technologies that could become standardized not just here but across the globe.

So imagine a possibility of actually being able to transfer property regardless of jurisdictional boundaries in much the same way when it comes to digital fiat currencies or digitized fiat currencies. There's been a number of efforts in order to explore this plane. There's been efforts by Singapore. I think recently there was an effort announced by Israel——

Mr. FOSTER. So they're actually——

Mr. WRIGHT. —to do it.

Mr. FOSTER. —functioning fiat currencies——

Mr. WRIGHT. I think it's in the proof-of-concept stage, but the thought is to represent traditional fiat currency in a digitized form and to replicate some of the innovations that we've seen with cryptocurrencies.

Mr. FOSTER. In terms of the supply chain application, it seems like the big beneficiary may be offshore places where the supply chain is sort of shaky and that there's a—we currently have a competitive advantage in the United States is that we have, you know, USDA and so on monitoring the egg supply chain. And I was wondering if that's something that you agree with or think that——

Mr. YIANNAS. I think there's opportunities in very developed supply chains. We see food safety scares happening in very developed nations, and so the benefits there apply. We know that very small tweaks or improvements in supply chains result in big benefits, and so we think the idea of a digitized food system, coupled with artificial intelligence and the Internet of Things, will allow us to run smarter, more efficient supply chains. So I think the benefits are for the entire—the food system is global in nature. I think the entire food system can benefit.

Mr. FOSTER. All right. Thank you. And yield back.

Chairman ABRAHAM. Thank you, Dr. Foster.

We've got a couple members that want follow-up questions, so we're going to be concise so—we've got limited time. Mr. Higgins, you're recognized.

Mr. HIGGINS. Thank you, Mr. Chairman.

Mr. Jaikaran, in your testimony you describe blockchain as not being a panacea technology or not appropriate solution for every industry or company in its management of data. Other than the ability to edit—inability to edit transactions—and I'm going to ask you, is that correct? It's——

Mr. JAIKARAN. Well, that might be one way, but yes, blockchains——

Mr. HIGGINS. Other than the ability to edit transactions, what are some of the risks to using a blockchain to record vital information and data? And I'm thinking within the governmental sector specifically.

Mr. JAIKARAN. Sure. Thank you for the question, sir. So in a government implementation, one of the big challenges with government is the user base. The user base is dispersed, unlike private sector that users and businesses might align. And in this particular example on technical savviness, government doesn't get to choose the technical savviness of its user base. So one of the bigger risks here is something we've already discussed, that a user loses their key and their ability to then transact on that public identity becomes a challenge.

So in addition to data not being able to be edited previously in the chain of a record was inserted inappropriately or inaccurately, the ability for a user to then conduct a new transaction might be difficult. Those are just two and briefly explaining it.

Mr. HIGGINS. What's your opinion regarding the inability to edit—it occurs to me for—for instance, regarding the Freedom of Information Act or public records request at the state or local level, if a blockchain—if the data within a blockchain cannot be edited, how can it be redacted?

Mr. JAIKARAN. That could be a potential problem. This goes back to—I discussed three attributes: business, legal, and technical. This might be both a legal and a business case when one is considering applying blockchain technology. Does that entity absolutely need an un-editable ledger of transactions?

The other side to that is maybe there's data that they do not publish to that blockchain, but that data is actually held on some other system that can be edited, but the record of that transaction, the record of that document being made or whatever that transaction might be—not all these transactions are financial—that that is then published to the blockchain so that there's——

Mr. HIGGINS. Okay. I don't think we've touched on that yet in this hearing. So there can be a marriage between a more secured system that's isolated from a blockchain and a blockchain system.

Mr. Cuomo, would you comment on that, sir?

Mr. CUOMO. Yes. We've implemented several systems that enable "right to be forgotten" by marrying exactly what you said together, two systems. One is a secure data store where a document or a piece of information is encrypted, and then a fingerprint or digital hash of that document is then placed on the blockchain. So what is being redacted is not the information but the cookie crumb that you put on the blockchain stays, right, so there's still evidence that something happened——

Mr. HIGGINS. So potentially——

Mr. CUOMO. —but the information to be deleted outside, yes.

Mr. HIGGINS. So potentially, a government system could be developed that would allow for the dissemination of public data through public information requests or Freedom of Information requests and still allow that government entity at the local, state, or federal level to redact data?

Mr. CUOMO. Yes.

Mr. HIGGINS. All right. Mr. Cuomo, you stated in your written testimony that an enterprise blockchain network is fault-tolerant. Can you briefly elaborate for us on that, please?

Mr. CUOMO. So in an enterprise blockchain like the Hyperledger Fabric, it's a modular architecture that supports a variety of consensus algorithms. And modern computer science supports a number of such algorithms that are fault-tolerant, and one of them is the Byzantine fault-tolerant algorithm that is emulated from the Byzantine general problem, which is back in the day I guess a general couldn't trust all his messengers, so he had to ensure that his orders were carried out even in the presence of bad actors. So MIT and others formulated algorithms that allow the operation of a general order to occur even in the presence of some carriers that may be, you know, bad actors.

Mr. HIGGINS. Fascinating. Mr. Chairman, I yield back. Thank you.

Chairman ABRAHAM. Thank you, Mr. Chairman.

Mr. Beyer.

Mr. BEYER. Thank you, Mr. Chairman.

Mr. Jaikaran? How do you pronounce that? We've been—we've——

Mr. JAIKARAN. Jaikaran.

Mr. BEYER. Jaikaran, yes. In your written testimony you say, quote, "Under key security, if the user's hard drive fails," which mine failed last year so—"or they forget or otherwise lose their private key"—just describing my wife—"they effectively lock the resource tied to the public key forever, inhibiting any other transaction with that asset." Is there not a danger if you've built up this blockchain that's gone on for years and is very long and somebody loses the private key?

Mr. JAIKARAN. Yes, that's precisely the example that I'm trying to articulate in my written testimony, yes, that there is a danger there.

Mr. BEYER. It sounds like a big danger. I just—I'm trying to think about how—if in my business I've spent years building a blockchain to record this immutable ledger of certain asset transfers, and all of a sudden, it's lost forever.

Mr. Cuomo?

Mr. CUOMO. Yes, nothing is foolproof. However, there are things you can do. For example, on the IBM blockchain is a service that implements this enterprise blockchain. We allow members of that block participating in that blockchain to store their keys in a crypto vault, right? Also, we enable governance to happen around, so you may you may choose not to join a network where one of the other members are not using such a vault, right? If they're just storing their keys on a laptop you may not say—you say, well, that—the risk is too high for me to join.

So governors of an enterprise blockchain could set the rules that can help mitigate sloppiness or carelessness like that. It won't eliminate but can help set a set of standards that would, you know, eliminate those sorts of problems.

Mr. BEYER. If you and I had a blockchain that we had built together for years and I lost my key, does that—my private key, does that then deny you access to it also?

Mr. CUOMO. Transactions that you and I are involved with are in jeopardy because whoever has your key can now see the transactions that you and I had conducted.

Mr. BEYER. Okay. All right. Thank you very much.

Mr. CUOMO. You're welcome.

Chairman ABRAHAM. Mr. Loudermilk?

Mr. LOUDERMILK. Thank you, Mr. Chairman. And I apologize for coming in late. I actually was in another committee hearing dealing with data security and financial services, and they just happen to be two areas of key interest of mine are going on at the same time.

I've often said recently that blockchain technology in my opinion of having 30 years in the IT industry is a potential solution to our cybersecurity risk that we have, which are significant and real. My concern is that the federal government, especially from the regulatory side, is always afraid of adopting something new because they don't understand it. And I'm seeing a lot of fear even among some of my colleagues because they're equating the technology behind cryptocurrency as the cryptocurrency itself, and I think this is something that we need to look at, we need to consider as a potential solution to our cybersecurity challenges we have right now.

Mr. Cuomo, am I off base with that or do you think that this is a potential solution, the technology, the blockchain technology is a solution?

Mr. CUOMO. I mean, it's not a silver bullet, but it certainly, if used in the right places, could help in a significant way. We talked about digital identity, and I think that's core to so many industries and government. So getting a handle in the right areas, not having honeypots of data—

Mr. LOUDERMILK. Right.

Mr. CUOMO. —doing digital rights management where end-users can actually manage their own data versus keeping it under one house, one honeypot, I think that will go a long way. We want to eliminate the problem, but it'll change the attack surface.

Mr. LOUDERMILK. Well, the way I've always looked at cybersecurity is it's impossible—as I think you said earlier, it's impossible to have an ultimately secured system. In fact, I remember when I was in the military and intelligence, a set of standards were set out. The standards were so stringent that once the system was built to actually meet the security standards, it was unusable because it was so slow.

I mean, there's two aspects of cybersecurity I've looked at. When I was—had my private business in the IT realm, we looked at security in the way of—it's—you can't ultimately secure yourself, it's to make it harder for the bad guy to get your data. It was like the two Georgians who went hiking in Alaska and a grizzly bear started chasing them. One of them sat down and put on his tennis shoes. The other one said, "You can't outrun the bear." He said, "I don't have to; I just have to outrun you." That's kind of the way cybersecurity is, to make you harder than the other guy.

And that's where I see the blockchain is it isn't the silver bullet, but it does make it much more difficult to find the honeypot. And in our environment today—and I have issues with the honeypots as well. Not only is there a honeypot, but because of our interest in data backup, we have multiple honeypots sitting out in clouds. And if you get into one, it's not that hard to backdoor to get in to another one somewhere.

The other aspect of cybersecurity—and anybody is welcome to weigh in on this one—is one of the areas we overlook is a key principle we had when I was in the military, which was you do not have to secure what you don't have. It's the amount of data that we are keeping sometimes that the government, through regulation, forcing businesses to keep data that isn't that valuable, they don't need to keep, or the government forcing industry to report data to the government, which in my opinion the government's the highest risk of anybody out there. Is that something that we should be addressing is the amount of data that we're requiring businesses to—and entities to keep on individuals? Anybody could weigh in on that one.

Dr. ROMINE. Well, from the NIST perspective, our cybersecurity approach has always been management of risk, something I know from your background you understand very well. And in this case, what you alluded to, this idea of data minimization is one aspect of managing risk. There's no question that that is an appropriate tool.

Other tools involve management of privacy risk, the idea of trying to ensure that you've satisfied the five functions that we talk about in the cybersecurity framework, the—identify your assets, protect them, detect when they've been compromised or attacked, respond to that, and then have a plan for recovery in the event that a breach actually occurs. Risk management is our approach.

Mr. LOUDERMILK. Well, I think to get to where we need to be is going to take a culmination of a lot of things, but I continue to see that the blockchain technology, because of how it disperses the data—I know there's some challenge, especially when it comes to law enforcement and some other aspects, but I think we do not need to be afraid of the new technology but figure out how to adopt it. And with that, Mr. Chairman, I yield back.

Chairman ABRAHAM. Thank you.

I recognize Mr. Perlmutter, who I understand is yielding to Dr. Foster?

Mr. PERLMUTTER. Yes, I am.

Mr. FOSTER. Yes. Thank you. I appreciate that, Mr. Perlmutter.

Let's see. The—one of the claims that's made about blockchain is that it's going to really solve a lot of the privacy problems, and probably the most direct—one of the biggest worries there are individual medical records. And could you walk me through how that might work? It seems to me that, you know, if you—even if you authenticate yourself to a doctor and he pulls your medical record, they exist in plaintext, unencrypted on his computer. If his computer is hacked, it's kind of game over and that your medical records will be for sale on the dark web in short order. And is there any blockchain-based solution to that fundamental problem of, you know, having your endpoint machine hacked, your cell phone hacked at the point that the user actually pulls up the clear direct data?

Mr. JAIKARAN. Thank you for the question, sir. So in the example that I talk about in my testimony of the provider maintaining that record, the record itself is still relying on the security measures of the provider, so if the provider's not implementing defense in depth, there's some other security strategies and an attacker, instead of attacking the blockchain, attacks the datastore of the provider, the record is still vulnerable. That would be the case today.

Mr. FOSTER. Yes. But there's no potential blockchain-based solution to that problem? If you're—if the terminal that you're displaying the data on has been hacked, you're sunk?

Mr. JAIKARAN. Not in any of the blockchain examples that I've seen implemented to date.

Mr. FOSTER. Okay. Yes, so that's—let's see. This is a question I guess related to NIST and all of the classified activity that we put a lot of taxpayer money into. Is there anything you can say about the level at which you communicate say the state of the art of quantum computing, which is very relevant? You're doing all this work, making assumptions about where quantum computing will be. You know, not all of the work in quantum computing is visible to everyone. Do you communicate at the very highest classified level or do you maintain a wall——

Dr. ROMINE. So in my laboratory—we don't do classified work on our campus. We're not involved in that at all. We do have people

who have access to information that can help inform us about the threat environment, and therefore give us tools where we can prioritize the kind of work that we do to have maximum impact.

In the area of quantum computing, I don't have any direct information that I have available to me in the classified setting—I can't divulge anything because I don't know anything——

Mr. FOSTER. All right. So you literally and your coworkers have no classified information? You can tell us everything you know? Or is there a repository inside NIST of, you know, secret stuff, state of the art of——

Dr. ROMINE. We have conversations with the folks in the intelligence community at classified levels periodically when there is threat information in the cybersecurity case, for example. If there's threat information that exists at the classified level that we may need to know to prioritize some of the work that we do, but the work that we do is entirely in the open and unclassified.

Mr. FOSTER. It's a tough—you know, a very tough thing to think through how you—we want to get this right. You know, I know that in my district, at Fermilab they're building qubits that will actually last more than a fraction of a millisecond because we lead the world in hi-Q superconducting resonators, which is one of the promising strategies, but, you know, this could immediately have big national security implications sort of instantaneously at the point that there's some breakthrough. And trying to understand, you know, how we handle that is tough and—okay.

So—and I guess that was the main question. I'll yield back my time.

Chairman ABRAHAM. Thank you, Dr. Foster.

Mr. Loudermilk?

Mr. LOUDERMILK. Thank you for the second round there, Mr. Chairman.

Mr. Cuomo, in your written testimony you discussed that we could thoughtfully insert blockchain in some appropriate projects already funded that would I believe you said "help ensure that we stay on the forefront of this transformative technology." Can you elaborate on what some of those already-funded projects may be and also where they wouldn't be appropriate to use blockchain?

Mr. CUOMO. Well, yes. I mean, I mentioned in my testimony the small—the SBIR, and that's basically the American seed funding. It's kind of their tagline. And I think there are many agencies from NIST to NASA that are getting funding for that, so I think stipulating as part of the funding and encouraging blockchain usage across whether it's sandbox development or, you know, land registries, I think going where there's already funding seems like a logical place to start.

Mr. LOUDERMILK. Okay. Thank you.

Chairman ABRAHAM. Mr. Perlmutter.

Mr. PERLMUTTER. Thank you.

And two quick questions to Mr. Wright and to Mr. Cuomo. First, could there be an infinite number of virtual currencies, question number one? Question number two, going back to my committee that I serve on in financial services, Terrorism and Illicit Finance, so how do we deal with circumventing sanctions by use of some sort of opaque currency? I mean, I don't want to be the—I want to

have a light touch, as you were talking about, Mr. Wright, but also I don't want to see al-Qaida or somebody else paid in cryptocurrencies and we can't find it. So I'll just—it's an open-ended question to the two of you.

Mr. WRIGHT. Thank you for the question. So with regard to the first question, can there be an infinite number of virtual currencies? I think the answer theoretically is yes. We've already seen an explosion in the number of virtual currencies that have been issued over the past four years. I think at last count there's at least 1,200 of them. In part that's because people just take existing virtual currency, the code base for it, and they just create a new version of it and make a couple tweaks and then release it.

With regard to illicit finance, on most current popular blockchains, they're actually highly traceable, so you can discern activity that's going on in the network because they rely on a peer-to-peer network so you actually have to convey information to all the members on the network. And so there's data that's leaked, and there's different analytics companies that have emerged that actually enable you to trace them.

There's a new generation of more anonymous virtual currencies that are now coming to the fore that rely on more advanced cryptography, and those present significant concerns, particularly with regard to the Bank Secrecy Act and the know-your-customer requirements, and other laws and regulations related to our payment systems.

In terms of how you regulate them, I think it actually raises a number of tricky and complex issues. One approach could actually be to try to steer activity towards regulated centralized intermediaries and exchanges where we can begin to uncover and collect some information about some of that activity in order to do more advanced network analysis to try to de-anonymize some of the activity on the network.

There's also been research that's been done with these more anonymous digital currencies in order to poke holes and see if there's any vulnerabilities, putting on your Tom Cruise hat from before, so I think that it's going to be a problem and it's going to continue to be a problem going forward.

Mr. PERLMUTTER. And just quickly, Mr. Cuomo.

Mr. CUOMO. And just quickly, while I like to believe that I'm a blockchain subject matter expert, I'm not a cryptocurrency expert, so I yield to Mr. Wright's comments.

Mr. PERLMUTTER. Okay. Thank you. I yield back. Thanks, Mr. Chairman.

Chairman ABRAHAM. Thank you, Mr. Perlmutter.

A very informative and important discussion today, very good. And moving forward, I'm going to ask a final question.

Oh, go ahead, Ms. Esty.

Ms. ESTY. Thank you very much. With a question about the personal keys, could you do biometric keys? Is that something that could be—which presumably is much harder to lose your own biometric key. If you've lost that, then you probably don't need to worry about blockchain.

Mr. JAIKARAN. Yes, while it would be possible to use a biometric identifier as a way to generate a key in the same way that your

iPhone does for unlocking your phone, you would then need some kind of biometric reader, so whatever computational device you're using would then have to do that. So I think that would be one of the limitations there is the hardware, not necessarily the crypto.

Chairman ABRAHAM. Thank you. So one final question. I'm going to kind of go back to Ms. Esty's first line of questioning. So moving forward with the continued utilization of blockchain technology, what do each of you see as the most significant or transformative application for business or the public sector, and how can this committee play a role in providing that support? Mr. Jaikaran, we'll start with you and then it's down the line.

Mr. JAIKARAN. So my research here in CRS hasn't really looked at what may be the most significant. I think there are some potential applications that may benefit particularly government applications and anything that can speed the efficiency of one transaction being validated from another. Unfortunately, the swath of available projects for that is just very wide at this point. So as the private sector, as researchers, and as agencies such as NIST continue to investigate this, as with internet technology, maybe something useful will bubble up that may be most applicable for government use.

Dr. ROMINE. We're just in the beginning stages, I think, of building our testbed to take a look at many different applications. If I were a betting man, I would say the application that really resonates is one that we haven't thought of yet.

Chairman ABRAHAM. Dr. Cuomo?

Mr. CUOMO. And I have to go back to digital identity. I think our digital lives in many cases are a mess. We are leaving parts of our digital life all over the place——

Chairman ABRAHAM. I would agree.

Mr. CUOMO. —and I think cleaning it up with some standards like what's happening with Sovrin Foundation I think could go a very long way and be an equal opportunity employer across government, industry, education, and more.

Chairman ABRAHAM. Mr. Yiannas?

Mr. YIANNAS. I don't know if it'll be the most but I think food is a very important——

Chairman ABRAHAM. I have to agree with that.

Mr. YIANNAS. —thing for society, and the idea that we could digitize food, it's one of the frontiers that hasn't been digitized, the learnings that we can get from that, the transparency that we can give to consumers, consumers increasingly concerned about food and where it comes from, we think will be important for society.

Chairman ABRAHAM. Thank you. Mr. Wright?

Mr. WRIGHT. I think public open blockchains are actually the major use case that will emerge, and they'll serve as a spine and a backbone for a number of different open protocols that transform a range of industries. And I think in terms of how we can encourage that here, I think regulatory clarity would be welcomed and helpful.

Chairman ABRAHAM. Okay. Well, look, thanks for a truly great discussion, from the Members' great questions, too.

So the record will remain open for two weeks for additional comments and written questions from Members. This hearing is adjourned. Thank you, gentlemen.

[Whereupon, at 12:09 p.m., the Subcommittees were adjourned.

Appendix I

Additional Material for the Record

LETTER SUBMITTED BY REPRESENTATIVE BEYER

JARED POLIS
2ND DISTRICT, COLORADO

1727 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-0602
(202) 225-2161
(202) 226-7840 (FAX)

website and email:
http://polis.house.gov

Congress of the United States
House of Representatives

VICE CHAIR AND PARLIAMENTARIAN
STEERING AND POLICY

PARLIAMENTARIAN OF THE WHIP

COMMITTEE ON
EDUCATION AND THE WORKFORCE
SUBCOMMITTEES:
RANKING MEMBER–EARLY CHILDHOOD, ELEMENTARY, AND SECONDARY EDUCATION
HIGHER EDUCATION AND WORKFORCE DEVELOPMENT

VICE RANKING MEMBER
COMMITTEE ON RULES

COMMITTEE ON ETHICS

February 14, 2018

The Honorable Barry Loudermilk
Chairman
Subcommittee on Oversight
House Science, Space, and
Technology Committee

The Honorable Donald Beyer
Ranking Member
Subcommittee on Oversight
House Science, Space, and
Technology Committee

The Honorable Barbara Comstock
Chairwoman
Subcommittee on Research and
Technology
House Science, Space, and
Technology Committee

The Honorable Daniel Lipinski
Ranking Member
Subcommittee on Research an
Technology
House Science, Space, and
Technology Committee

Dear Chairman Loudermilk, Chairwoman Comstock, Ranking Member Beyer and Ranking Member Lipinski,

As co-chairs of the Congressional Blockchain Caucus, we commend you in holding this important hearing titled, "*Beyond Bitcoin: Emerging Applications for Blockchain Technology.*" Blockchain technology was introduced to the world as the underlying technology that gave bitcoin its unique properties-it allows secure peer-to-peer payments without an intermediary. While Bitcoin relies on blockchain technology; blockchain does not rely on Bitcoin to exist. The Congressional Blockchain Caucus has been hosting briefings that explore how blockchain technology can be used by private industries and the public sector to solve complex problems.

What is blockchain technology?

The technology underlying the Bitcoin is called the blockchain. Blockchain is a peer-to-peer decentralized ledger of timestamped transactions.[1] Cryptography ensures that all computers in the network have constantly updated and verified records of the transactions.[2] Because of the distributed nature of the blockchain, the transactions are more secure, more reliable, and cannot be altered by one entity after appearing on the blockchain.

The private and public sector see blockchain technology as a way to improve data security, minimize or eliminate third party intermediaries, make transactions faster and improve

---

[1] *Blockchain 101*, Coincenter, https://coincenter.org/learn (accessed on Feb. 11, 2018).

[2] Jerry Brito and Angela Castilo, *Bitcoin: A Primer for Policymakers*, pg. 6 (2016).

PRINTED ON RECYCLED PAPER

transparency. But in order to realize these benefits in other applications, it is important to consider whether blockchain is the appropriate technology.

The most unique property of the Bitcoin blockchain is that the software is run on many computers at the same time, rather than one central server and the network of computers works together to verify the ledger.[3] This is called "decentralized consensus computing," which has the ability to be transformative and truly disruptive. Bitcoin and other cryptocurrencies rely on this type of public or permission-less blockchains.

Permission-based distributed ledgers, on the other hand, utilize the same the consensus computing, but the consensus and access is limited to specified actors. These types of distributed ledgers are favored by those in the financial services sector that may only want to share certain transaction information.

Whether permission-based distributed ledgers or public blockchains, this type of technology has the ability to dramatically change business or government operations. But as Congress explores this type of technology, it is important that we do not stifle innovation or take a position on whether open or permission-based is better. Markets, consumers, technologists and businesses should decide which technologies are best suited for the various applications.

Emerging Applications in the Public Sector

At all levels, government entities are also exploring how best to utilize blockchain technology.

In 2016, the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology held a blockchain challenge, asking participants to explore how blockchain technology could be utilized in health and health IT to protect, manage and exchange electronic health information.[4] The Department chose 15 winners, with topics ranging from how to manage electronic health records with blockchain to how to reduce improper or over prescriptions.

The U.S. Postal Service's Inspector General explored how the Postal Service could utilize blockchain for supply chain management in order to improve package and mail delivery, used for identity management and verification, or even for international electronic money transfers.[5]

---

[3] Peter Van Valkenburgh, *Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet*, pg. 10 (2016).

[4] Dept. of Health and Human Services, Office of the National Coordinator for Health Info.Tech.; Announcement for Requirements and Registration for "Blockchain and Its Emerging Role in Healthcare and Health-related Research (2016), accessed at https://s3.amazonaws.com/public-inspection.federalregister.gov/2016-16133.pdf

[5] Office of the Inspector General, United States Postal Service, *Blockchain Technology: Possiblities for the U.S. Postal Service* (2016), https://www.uspsoig.gov/sites/default/files/document-library-files/2016/RARC-WP-16-001.pdf.

In Colorado, SB 10-086, the Cyber Coding Cryptology Act was introduced to encourage the Office of Information Technology, the Department of State and the Department of Regulatory Agencies to review use cases for blockchain technology and encryption technologies throughout the state. The goal of this legislation is to explore how blockchain can be effectively used at the state level to improve state services.

South Burlington, Vermont, is exploring the use of blockchain technology for recording land registration and ownership. This is an exciting area where blockchain could possibly reduce costs for storing land management data and improve tracking of land ownership to minimize titling issues.

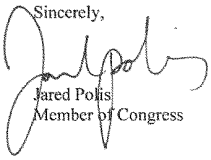
These are just a few examples of where governments have recognized the potential of blockchain technology and are exploring ways to incorporate it into their functions.

Congress' Role to Encourage Innovation in Technology

As this Committee and others explore blockchain technology and the applications that are utilizing the technology, it is important that we are able to separate the software from the outcomes. Regulation should be technology neutral so not to stifle innovation. Instead, regulation should be focused on how to incorporate blockchain technology into the regulatory structure to achieve important public policy goals, like combating money laundering or improving transparency in financial transactions. Further, Congress should encourage regulators and agencies to explore the use of blockchain technology and allow for experimentation.

This is a very important topic for the Science Committee to explore and I appreciate the opportunity to submit a statement for this hearing. If you have any questions, please contact Hilary Gawrilow (hilary.gawrilow@mail.house.gov) in my office.

Sincerely,



Jared Polis
Member of Congress