

**LEVERAGING BLOCKCHAIN TECHNOLOGY
TO IMPROVE SUPPLY CHAIN MANAGEMENT
AND COMBAT COUNTERFEIT GOODS**

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

MAY 8, 2018

Serial No. 115-57

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

30-320PDF

WASHINGTON : 2018

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

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

| | |
|------------------------------|--------------------------------|
| FRANK D. LUCAS, Oklahoma | EDDIE BERNICE JOHNSON, Texas |
| DANA ROHRBACHER, California | ZOE LOFGREN, California |
| MO BROOKS, Alabama | DANIEL LIPINSKI, Illinois |
| RANDY HULTGREN, Illinois | SUZANNE BONAMICI, Oregon |
| BILL POSEY, Florida | AMI BERA, California |
| THOMAS MASSIE, Kentucky | ELIZABETH H. ESTY, Connecticut |
| RANDY K. WEBER, Texas | MARC A. VEASEY, Texas |
| STEPHEN KNIGHT, California | DONALD S. BEYER, JR., Virginia |
| BRIAN BABIN, Texas | JACKY ROSEN, Nevada |
| BARBARA COMSTOCK, Virginia | CONOR LAMB, Pennsylvania |
| BARRY LOUDERMILK, Georgia | JERRY MCNERNEY, California |
| RALPH LEE ABRAHAM, Louisiana | ED PERLMUTTER, Colorado |
| DANIEL WEBSTER, Florida | PAUL TONKO, New York |
| JIM BANKS, Indiana | BILL FOSTER, Illinois |
| ANDY BIGGS, Arizona | MARK TAKANO, California |
| ROGER W. MARSHALL, Kansas | COLLEEN HANABUSA, Hawaii |
| NEAL P. DUNN, Florida | CHARLIE CRIST, Florida |
| CLAY HIGGINS, Louisiana | |
| RALPH NORMAN, South Carolina | |

SUBCOMMITTEE ON OVERSIGHT

RALPH LEE ABRAHAM, LOUISIANA, *Chair*

| | |
|------------------------------|--------------------------------|
| BILL POSEY, Florida | DONALD S. BEYER, Jr., Virginia |
| THOMAS MASSIE, Kentucky | JERRY MCNERNEY, California |
| BARRY LOUDERMILK, Georgia | ED PERLMUTTER, Colorado |
| ROGER W. MARSHALL, Kansas | EDDIE BERNICE JOHNSON, Texas |
| CLAY HIGGINS, Louisiana | |
| RALPH NORMAN, South Carolina | |
| LAMAR S. SMITH, Texas | |

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. BARBARA COMSTOCK, Virginia, *Chair*

| | |
|----------------------------|--------------------------------|
| FRANK D. LUCAS, Oklahoma | DANIEL LIPINSKI, Illinois |
| RANDY HULTGREN, Illinois | ELIZABETH H. ESTY, Connecticut |
| STEPHEN KNIGHT, California | JACKY ROSEN, Nevada |
| DANIEL WEBSTER, Florida | SUZANNE BONAMICI, Oregon |
| JIM BANKS, Indiana | AMI BERA, California |
| ROGER W. MARSHALL, Kansas | DONALD S. BEYER, JR., Virginia |
| LAMAR S. SMITH, Texas | EDDIE BERNICE JOHNSON, Texas |

CONTENTS

May 8, 2018

| | |
|-----------------------|-----------|
| Witness List | Page 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 |
| Written Statement by Representative Eddie Bernice Johnson, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives | 8 |
| Written Statement by Representative Donald S. Beyer, Jr., Ranking Member, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives | 10 |
| Written 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 by Representative Daniel Lipinski, Ranking Member, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives | 14 |

Witnesses:

| | |
|---|----|
| Dr. Douglas Maughan, Cyber Security Division Director, Science and Technology Directorate, U.S. Department of Homeland Security | |
| Oral Statement | 16 |
| Written Statement | 19 |
| Mr. Robert “Bob” Chiaviello, IPR Counsel, Nuby Law | |
| Oral Statement | 27 |
| Written Statement | 29 |
| Mr. Michael White, Head of Global Trade Digitization, Maersk | |
| Oral Statement | 50 |
| Written Statement | 53 |
| Mr. Chris Rubio, VP Global Customs Brokerage Staff, UPS | |
| Oral Statement | 57 |
| Written Statement | 60 |
| Discussion | 65 |

Appendix I: Answers to Post-Hearing Questions

| | |
|---|----|
| Dr. Douglas Maughan, Cyber Security Division Director, Science and Technology Directorate, U.S. Department of Homeland Security | 84 |
| Mr. Robert “Bob” Chiaviello, IPR Counsel, Nuby Law | 87 |
| Mr. Michael White, Head of Global Trade Digitization, Maersk | 89 |
| Mr. Chris Rubio, VP Global Customs Brokerage Staff, UPS | 91 |

**LEVERAGING BLOCKCHAIN TECHNOLOGY
TO IMPROVE SUPPLY CHAIN MANAGEMENT
AND COMBAT COUNTERFEIT GOODS**

TUESDAY, MAY 8, 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

***Leveraging Blockchain Technology to Improve Supply Chain
Management and Combat Counterfeit Goods***

Tuesday, May 8, 2018

10:00 a.m.

2318 Rayburn House Office Building

Witnesses

Dr. Douglas Maughan, Cyber Security Division Director, Science and
Technology Directorate, Department of Homeland Security

Mr. Robert Chiaviello, IPR Counsel, NUBY Law

Mr. Michael White, Head of Global Trade Digitization, A.P. Moller – Maersk
Transport & Logistics

Mr. Christopher Rubio, Vice President of Global Customs Brokerage Staff,
United Parcel Service

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

HEARING CHARTER

May 2, 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: *Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods*.

The Subcommittees on Oversight and Research and Technology will hold a joint hearing entitled *Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods* on Tuesday, May 8, 2018, at 10:00 a.m. in Room 2318 of the Rayburn House Office Building.

Hearing Purpose:

The purpose of this hearing is to highlight potential and proven applications of blockchain and distributed ledger technology in shipping, logistics, and customs, with an emphasis on supply chain management. The hearing will focus on how this technology can be leveraged to provide greater supply chain visibility and combat the distribution of counterfeit products.

Witness List:

- **Dr. Douglas Maughan**, Cyber Security Division Director, Science and Technology Directorate, U.S. Department of Homeland Security
- **Mr. Robert “Bob” Chiaviello**, IPR Counsel, Nuby Law
- **Mr. Michael White**, Head of Global Trade Digitization, Maersk
- **Mr. Chris Rubio**, VP Global Customs Brokerage Staff, UPS

Staff Contact:

For questions related to the hearing, please contact Tom Connally or Travis Voyles 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, and welcome to today's hearing entitled "Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods." I'll recognize myself for five minutes for an opening statement.

Good morning again. Welcome to today's joint Oversight and Research and Technology Subcommittee hearing, "Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods." Today's hearing will highlight potential applications of blockchain technology in shipping, logistics, and customs, emphasizing supply chain management. A focus today will be how this technology can be leveraged to a greater visibility into the supply chain and how the technology can be used to combat the distribution of counterfeit products.

We will hear from government and private-sector experts about blockchains potential to improve the security of our systems and how it can ensure customers and the companies alike, that the products and services being used are verified.

The Science Committee continues to engage in oversight of emerging forms and applications of technology, just like the discussion that we—will occur on blockchain today. We recognize that these technologies can benefit both the public and private sectors and seek to understand what can be done to ensure that this technology is appropriately leveraged in an efficient and productive manner.

Through ensuring reliability, increasing productivity, and securing systems and data, the application of blockchain technology is an area in which there is much to learn. While the applications for blockchain technology are continuously increasing, this hearing is an opportunity to learn more about its specific use in supply chain management. Today's witnesses can provide valuable insight into how blockchain can enhance security and be leveraged outside of the private sector to improve government efficiency.

We must also recognize that—the barriers faced by the private sector in leveraging blockchain technology in order to fully realize its potential benefits. By hearing from individuals today that are taking part in ongoing and proactive efforts within the private sector to utilize blockchain technology in different areas of their business models, we can gain a better understanding of what, if anything, industry needs from the government.

I want to thank Mr. White for being here to represent Maersk, and Mr. Rubio representing UPS. These companies are presently engaged in important case studies using this technology. We look forward to learning about those efforts.

Additionally, Mr. Chiaviello is here today to do—detail some of the counterfeiting and business issues companies like Luv N' Care are experiencing. Baby care products are some of the most important on the market. We must be able to verify the authenticity of these goods. There is a potential role emerging for technologies like blockchain to address these global supply chain safety issues.

The committee will continue to prioritize issues like verification and overall cybersecurity. We hope venues like today's hearing will help provide a better understanding of the issues our private industries are facing and how they are utilizing emerging technologies. This knowledge can better inform the Committee on how the application of blockchain technology could potentially bolster private companies' and the federal government's cybersecurity weaknesses.

Dr. Maughan, we appreciate you being here today to provide more insight into the role DHS has played in utilizing this emerging technology. DHS Science and Technology Directorate is in a unique position to provide valuable insight and services as a useful role in exploring a broader understanding and application of the technology in areas directly related to shipping, logistics, and customs.

Additionally, through the many projects and ventures it supports, DHS has the ability to effectively identify the potential for blockchain technology and address how the federal government could benefit. These potential solutions could help secure data and enhance our national security.

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

[The prepared statement of Chairman Abraham follows:]



COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
May 8, 2018

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

Statement by Chairman Ralph Abraham (R-La.)

Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods

Chairman Abraham: Today's hearing will highlight potential applications of blockchain technology in shipping, logistics and customs, emphasizing supply chain management. A focus today will be how this technology can be leveraged to provide greater visibility into the supply chain and how the technology can be used to combat the distribution of counterfeit products. We will hear from government and private-sector experts about blockchain's potential to improve the security of our systems and how it can ensure customers and the companies alike, that the products and services being used are verified.

The Science Committee continues to engage in oversight of emerging forms and applications of technology, just like the discussion that will occur on blockchain today. We recognize that these technologies can benefit both the public and private sectors, and seek to understand what can be done to ensure that this technology is appropriately leveraged in an efficient and productive manner. Through ensuring reliability, increasing productivity, and securing systems and data, the application of blockchain technology is an area in which there is much to learn.

While the applications for blockchain technology are continuously increasing, this hearing is an opportunity to learn more about its specific use in supply chain management. Today's witnesses can provide valuable insight into how blockchain can enhance security and be leveraged outside of the private sector to improve government efficiency.

We must also recognize the barriers faced by the private sector in leveraging blockchain technology in order to fully realize its potential benefits. By hearing from individuals today that are taking part in ongoing and proactive efforts within the private sector to utilize blockchain technology in different areas of their business models, we can gain a better understanding of what, if anything, industry needs from the government.

I want to thank Mr. White for being here to represent Maersk, and Mr. Rubio representing UPS. These companies are presently engaged in important case studies using this technology. We look forward to learning about those efforts. Additionally, Mr. Chiaviello is here today to detail some of the counterfeiting and business issues companies like Luv n' Care are experiencing. Baby care products are some of the most important on the market. We must be able to verify the authenticity of these goods. There is a potential role emerging for technologies like blockchain to address these global supply chain safety issues.

The committee will continue to prioritize issues like verification and overall cybersecurity. We hope venues like today's hearing will help provide a better understanding of the issues our private industries are facing and how they are utilizing emerging technologies. This knowledge can better inform the committee on how the application of blockchain technology could potentially bolster private companies' and the federal government's cybersecurity weaknesses.

Dr. Maughan, we appreciate you being here today to provide more insight into the role the Department of Homeland Security (DHS) has played in utilizing this emerging technology. DHS Science and Technology Directorate is in a unique position to provide valuable insight and serves a useful role in exploring a broader understanding and application of the technology in areas directly related to shipping, logistics and customs. Additionally, through the many projects and ventures it supports, DHS has the ability to effectively identify the potential for blockchain technology and address how the federal government could benefit. These potential solutions could help secure data and enhance our national security.

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

###

[The prepared statement of Ms. Johnson follows:]

OPENING STATEMENT

Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space & Technology
Subcommittee on Oversight

Subcommittee on Research and Technology
*"Leveraging Blockchain Technology to Improve Supply
Chain Management and Combat Counterfeit Goods"*
May 8, 2018

Thank you Chairman Abraham and Chairwoman Comstock.

In February, we held a joint subcommittee hearing on the "emerging applications for blockchain technology." At that hearing, I stressed the need to "go beyond the hype and understand the real limitations of blockchain technology." And today, I want to again stress the need to go beyond the blockchain hype. While I recognize the great potential of blockchain technology, blockchain has become a buzzword, and a splashy marketing tool. The name "Blockchain" has been slapped on solutions that do not technically meet the specifications of a blockchain. Blockchain technology is also being offered as the solution to problems when much simpler methods would be sufficient, or better. I hope that today's hearing will discuss these issues.

But blockchain is not amongst the pressing issues that this Committee should be having TWO hearings on in less than THREE months. The Oversight subcommittee, and the Science Committee overall, has failed to look into serious allegations of wrongdoing by the current EPA Administrator Scott Pruitt. This is unacceptable. Just a sampling of Mr. Pruitt's actions:

Mr. Pruitt rented a room in an energy lobbyist wife's Capitol Hill condominium for well-below market rate. Contrary to Mr. Pruitt's initial public assertions, the lobbyist conducted business with EPA, even meeting, on behalf of a client, with Mr. Pruitt at EPA headquarters. Additionally, according to a recent *New York Times* article, this lobbyist later asked Mr. Pruitt to appoint three people to the EPA's Science Advisory Board. This request was at the behest of one of the lobbyist's clients.

Another example—the Government Accountability Office (GAO) determined that the EPA broke the law when it purchased a \$43,000 soundproof phone booth for Mr. Pruitt without the necessary Congressional notification and appropriation.

Additionally, Administrator Pruitt uses three different EPA email addresses in addition to his official email address. There have been indications that some of these e-mails are not checked for documents responsive to Freedom of Information Act (FOIA) requests.

This is just a sampling of Mr. Pruitt's alleged wrongdoing. There are now 11 federal investigations into alleged wrongdoing by Mr. Pruitt, but no action from this Committee. This is unacceptable.

Beyond the current investigations of Mr. Pruitt, there are further areas of necessary inquiry. Mr. Pruitt has repeatedly acted to undercut the role of science in informing EPA's rulemaking. Mr.

Pruitt has taken steps to remove independent scientists from the Agency's science advisory panels and stocked the panels with industry representatives and scientists funded by industry interests. This undermines the scientific integrity of the EPA, as sound objective scientific data is supplanted by industry-focused information.

Mr. Pruitt has moved the review of potential EPA grant awards away from scientific experts, and into the hands of political appointees. Allegedly, the individual responsible for vetting these scientific grants has no scientific background or expertise. This undermines the integrity of EPA-funded studies, as it appears that politics, and not science, has taken precedence in EPA's grant decision-making process.

It is time this Committee began fulfilling its obligation to examine this Administration and hold bad actors accountable when they engage in unsound, unethical, or illegal activities.

Mr. Chairman, I stand ready to join with any legitimate efforts to hold members of the Executive Branch accountable for their actions, as this Committee has done with past Administrations when necessary. If even a fraction of the many allegations are true, Mr. Pruitt has repeatedly violated the public trust, and that should not be ignored.

I yield the balance of my time.

[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 Hearing

Subcommittee on Oversight

Subcommittee on Research and Technology

*Leveraging Blockchain Technology to Improve Supply Chain Management
and Combat Counterfeit Goods*

May 8, 2018

Thank you, Chairman Abraham and Chairwoman Comstock.

As I said at the last hearing we had on Blockchain in February, I believe Blockchain technologies offer tremendous promise and potential pitfalls. Cryptocurrencies and financial services based on Blockchain may result in more secure and efficient transactions. Blockchain technologies may also reduce costs in supply chain management, improve the security of healthcare records, and the verifiability of government issued documents, such as passports.

True Blockchain technologies are composed of three core components, a distributed peer-to-peer network, the use of advanced cryptography, and a consensus mechanism for determining the contents of new blocks or data added to the Blockchain. As today's witness from the Department of Homeland Security (DHS) has noted, many so-called Blockchain projects fail that test and most organizations don't need a Blockchain to enhance their security, transparency or efficiency.

Blockchain is not a solution to every problem. There is considerable hype and confusion surrounding Blockchain. High-tech company insiders have acknowledged that internally some IT companies are simply rebranding database projects with Blockchain-related terms to feed off this hype and position themselves into the center of this Blockchain buzz.

Some examples of this are extreme. In December, the Long Island Iced Tea Corporation, which produces non-alcoholic beverages, announced they were changing their name to the Long Blockchain Corporation, saying they wanted to partner with Blockchain investors. The company's shares rose nearly 300% as a result. The buzz soon wore off, the company found no Blockchain partners, and the company was recently delisted from the NASDAQ stock exchange.

The ability to use the Science Committee to highlight true Blockchain and other emerging technologies is both powerful and positive. I applaud those efforts. However, we should also ensure that the Committee does not feed the Blockchain buzz in inappropriate ways or add to the hype or confusion about this technology. Leveraging technology to make trade more efficient or to curtail illicit transactions is a worthy effort and when it comes to technical solutions to these problems as we will hear from some of our witnesses today we have a legitimate role in investigating those efforts. However, our Committee should not serve as a forum for trade disputes and we should not confuse trade issues or legal claims with technical issues. I believe issues revolving around counterfeit goods, for instance, are better left to the courts or other Congressional Committees with jurisdiction over those matters.

I *do* believe, however, that we should use the legitimate oversight authority of this Committee to investigate technologies that can help improve our democratic processes and ensure the sanctity and security of our election infrastructure. The Science Committee has a clear role in overseeing standards used for voting machines, for instance, and we should fulfill our oversight obligation to the American public by helping to ensure the integrity of our election infrastructure. We also have an obligation to hold public officials accountable for their mismanagement and unethical actions. Sadly, during this Administration, the Science Committee has failed to do either.

This Committee has failed in its oversight efforts to hold the leaders of this Administration accountable to the public, as we have seen in the case of Administrator Pruitt, who has still not testified before Committee nor been invited. It has also failed to ensure that the technologies we utilize in our most important democratic process – holding free and fair elections – are sound, secure and reliable. As I have now said for the *sixth* time since October, we are willing to help the Majority investigate this issue in a nonpartisan manner that will benefit the public and make our Republic stronger and more secure from foreign influence operations and cybersecurity attacks against our election infrastructure. I once again implore the leadership of this Committee, once again, to stop ignoring these important issues and start addressing them in a meaningful way.

I do look forward to hearing from all of our witnesses today regarding the positive benefits of employing true Blockchain technologies, but I hope that we can turn our attention to these other critically important topics in the near future.

Thank you.

[The prepared statement of Mrs. Comstock follows:]



COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
May 8, 2018

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

Statement by Chairwoman Barbara Comstock (R-Va.)

Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods

Chairwoman Comstock: In February, we heard from witnesses about the non-bitcoin applications of blockchain technology during a joint hearing. While we learned much from that panel, it became evident that there are many more potential applications of this technology to examine. Today we delve into some of the potential and proven applications of this ledger technology, namely in the areas of shipping, logistics and customs.

The global marketplace has added complexity to modern supply chains and complicated their effective management. The supply chain of a given product can span several stages and geographical locations.

Modern supply chains typically consist of several individuals and entities, involve multiple payments and invoices and can take months for a product to move from beginning to end.

As manufacturing becomes increasingly more globalized in nature, managing modern supply chains will become increasingly complex.

While this has implications for the speed, efficiency and accuracy of goods ordered, a larger concern is the authenticity of an ordered item as counterfeit products increasingly saturate the modern consumer market.

According to one of our witnesses today, each year, more than \$16 trillion worth of products cross international borders. Yet by some accounts, counterfeit and pirated goods are expected to siphon \$4.2 trillion from the global economy by 2022.

Despite living in an age where we can have almost anything delivered in 24 hours—or less—we still deal with such questions of accuracy and authenticity when it comes to the goods ordered.

It's a side effect of having access to an international supply chain as we can never be quite sure of the origin of the product purchased.

Today's hearing will provide some insight on how blockchain technology may help tilt the scales in favor of the consumer with better tracking and transparency of the supply chain.

Maersk for example, represented at our hearing today, began a collaboration with IBM earlier this year to digitize the global supply chain.

A few months ago UPS, also represented today, announced it would join the Blockchain in Transport Alliance. The alliance provides a "forum for the development of blockchain technology standards and education for the freight industry," with hopes of jumpstarting standards development for the shipping industry by implementing a secure blockchain system.

Even the federal government is involved as we will hear about programs within the Department of Homeland Security's Science and Technology Directorate relative to blockchain technology.

I hope these efforts will prove fruitful. When consumers are faced with a deal that seems too good to be true, they should feel confident to have found a deal that is a bargain and not a counterfeit product.

###

[The prepared statement of Mr. Lipinski follows:]

OPENING STATEMENT

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

House Committee on Science, Space, and Technology Hearing
Subcommittee on Oversight
Subcommittee on Research and Technology
*Leveraging Blockchain Technology to Improve Supply Chain Management
and Combat Counterfeit Goods*
May 8, 2018

Thank you, Chairman Abraham and Chairwoman Comstock, for holding this hearing on current and potential supply chain management applications for blockchain technology. And thank you to the witnesses for being here this morning to share your expertise with us as we continue to examine what types of challenges are most effectively addressed with blockchain technology.

Just this past February, this Committee held a hearing on emerging applications of blockchain technology. That hearing gave us a chance to better understand the promises, and limitations, of blockchain. As I and several of my colleagues noted then, the potential for blockchain technologies to provide more secure, reliable, transparent information makes it an attractive option in many sectors of the economy. Supply chain management is one sector that is embracing blockchain technologies; in many circumstances, efficiency, transparency, and security seem to be improving as a result.

As a Member of both the Science Committee and the Transportation Committee, I am interested in applications of blockchain for logistics management, which is the component of supply chain management focused on how to move raw materials, intermediate products, and finished goods from their origins to their destinations. Last week, several major car companies launched a blockchain research group for the automotive industry. I look forward to hearing from the witnesses about how the maritime, aviation, rail, and surface transportation sectors interface with blockchains for logistics and supply chain management.

The Federal government is supporting blockchain technology through research and development work at several agencies, including the National Institute of Standards and Technology – or NIST – and the National Science Foundation. NIST has played an important role in supporting the fundamental research and developing the standards for the underlying technologies that blockchain is built upon. In a recent publication, the agency highlighted several important research areas that are critical for blockchain's wide-scale deployment, including new cryptographic methods and common standards and protocols. Advances in these areas will help implement appropriate blockchain solutions across different sectors and for different purposes.

As we will hear today, the Department of Homeland Security's Science and Technology Directorate is supporting R&D to use blockchain to increase the security and reliability of the chain of custody for goods moving over our borders and across our oceans with our international trading partners. This is one of many critical ways in which this directorate keeps us safe and I want to take a moment to comment on its leadership. It is important that we have permanent leadership at the top levels of this office, yet the title of the head person has changed from "Acting Under Secretary for Science and Technology" to "Senior Official Performing the Duties of the Under Secretary for Science and Technology." I am concerned that

this name change implies that a long-term appointee is not anticipated anytime soon, and I encourage the Administration to act swiftly on naming a permanent leader to this office.

Supporting emerging technologies, such as blockchain, that have the potential to make our economy more efficient, reliable, and safe is important. In addition to improving the efficiency and sustainability of businesses and governments, the blockchain industry is creating new companies and jobs around the country. According to Forbes, Chicago ranks fourth in the country for blockchain jobs; last year, the State of Illinois helped launch a blockchain incubator there to help launch and grow companies. This is an important trend and one that federal, state, and local governments should continue to support.

At the same time, we have to distinguish valid areas for blockchain technology's use from misguided or inappropriate deployments. For example, while blockchain may make sense for complex, global supply chains made up of many parties with little knowledge or trust of one another, it may offer fewer benefits to regionally concentrated manufacturing consortia consisting mainly of small producers. I look forward to hearing from our expert panel regarding how the supply chain management sector can appropriately apply blockchain technologies.

I want to thank the witnesses again for being here. I yield back.

Chairman ABRAHAM. We're going to recognize our witnesses now. Our first witness today is Dr. Douglas Maughan, Director of the Cyber Security Division of the Science and Technology Directorate at the Department of Homeland Security. Dr. Maughan previously worked at the National Security Agency from 1987 to 1999 as a Senior Computer Scientist before moving to DARPA to work as a Program Manager. In 2003, he joined the Department of Homeland Security as a Program Manager and was promoted to Division Director in 2010. He holds two bachelor's degrees from Utah State University in computer science and applied statistics, a master's degree in computer science from Johns Hopkins University, and a doctorate in computer science from the University of Maryland, Baltimore County.

Our second witness is Mr. Bob Chiaviello, an IPR Counsel at Nuby Law. Mr. Chiaviello has practiced intellectual property law for 37 years starting at Pennie & Edmonds in 1980. After a brief stint with IBM, he joined Baker Botts in 1990. In 2002, Mr. Chiaviello joined Fulbright & Jaworski as a partner and worked there until 2011. He received his bachelor's degree from Washington and Lee University and his juris doctor from the John Marshall Law School.

Our next witness is Mr. Michael White, head of the Global Trade Digitalization at Maersk. Mr. White has worked at Maersk since 2007, first as a Managing Director at Maersk Holding. He then became Managing Director at Maersk Line before becoming the head of Global Trade Digitization in 2017. He received a bachelor's degree from Virginia Wesleyan University and also studied at Harvard Business School and the International Institute for Management Development business school in Lausanne, Switzerland.

Our final witness is Mr. Christopher Rubio, Vice President of Global Customs Brokerage Staff at United Parcel Services. Mr. Rubio holds a bachelor's degree in accounting from Pace University and an MBA in finance from Rutgers University. He has worked for UPS since 2004, first as Department Manager for the Midmarket Sales Team. He then became the Department Manager for UPS Trade Management Services before joining the Global Customs Brokerage System Group.

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

**TESTIMONY OF DR. DOUGLAS MAUGHAN,
CYBER SECURITY DIVISION DIRECTOR,
SCIENCE AND TECHNOLOGY DIRECTORATE,
U.S. DEPARTMENT OF HOMELAND SECURITY**

Dr. MAUGHAN. Chairman Abraham and distinguished Members of the Oversight and Research and Technology Subcommittees, thank you for inviting DHS to speak with you today. I will be sharing important aspects of how the Department of Homeland Security Science and Technology Directorate is using blockchain technologies in research and development and working with department missionaries to integrate the innovative technology into everyday use.

As the R&D arm of DHS, S&T develops the tools, technologies, and knowledge products for DHS operators and state and local first

responders, ensuring that R&D coordination across the Department to develop solutions for the needs of today and tomorrow. S&T partners with federal agencies, industry, academia, and international governments to create and test real-world solutions that help the Nation's homeland security officials defend against, respond to, mitigate, and recover from all hazards and threats in a realistic time frame.

Blockchains offer promise, as witnessed by the rapid growth of interest across government and private sector. From a government perspective, the technology holds potential for enhanced transparency and auditing of public service operations, greater supply chain visibility to combat the distribution of counterfeit products, and automation of paper-based processes to improve delivery of services to organizations and citizens.

There are many types of blockchains with varying degrees of support of classic security principles such as confidentiality, integrity, and availability, as well as support of privacy principles such as pseudonymity and selective disclosure. Analysis to determine if a particular blockchain supports these security and privacy considerations is often nonexistent and/or not readily available. There remain other challenges with blockchain technology, particularly a lack of support for standards that may limit the growth and availability of a competitive marketplace of interoperable, cost-effective, and innovative solutions for both government and industry.

Certainly, private industry is leading the way in blockchain development, as many see it as a key competitive advantage. Government must be informed and ensure blockchain technology, as it evolves, supports standardized approaches for security privacy and data exchange to create efficiencies and enhance the public good. Government must also consider leadership opportunities within the broader community and partner with industry to bring solutions to market.

Blockchain technologies are an integral part of several ongoing S&T research efforts with both DHS components and industry partners. We're exploring many issues, including the development of best practices and decision criteria on when and how to implement the blockchain technologies, understanding the support for security and privacy principles in commercial blockchain implementations, developing specifications to ensure standardized approaches for decentralized identifiers, defining interoperable data formats using verifiable credentials, and identifying scalable and usable approaches to decentralized key management systems.

DHS S&T is also supporting the development of globally available specifications as a precursor to standards, which are open, royalty-free, and free to implement to ensure interoperability across systems, while ensuring there is no vendor lock-in. We are doing this through organizations like the World Wide Web Consortium and the Organization for the Advancement of Structured Information Standards.

Within DHS, the U.S. Customs and Border Protection organization has been the most active operational component to partner with S&T on the use of blockchain technologies for its mission. Our ongoing engagements with CBP include a proof-of-concept deployment with the Border Patrol to evaluate how blockchain technology

can ensure the authenticity and integrity of imagery data collected from cameras, both fixed and mobile; conducting analysis of alternatives and feasibility studies to understand the potential benefits and challenges for facilitating and enhancing international passenger travel; and conducting proof-of-concept deployments in partnership with CBP's Office of Trade and Office of Trade Relations that are directly focused on applications of blockchain to shipping, logistics, and customs.

Blockchains are moving rapidly from hype to reality in the application domain areas where DHS S&T is currently working. We believe our careful and considered approach benefits not just DHS but everyone who is considering the use of a blockchain technology by ensuring that there are multiple vendors with interoperable solutions from which the government can choose.

Thank you again for your committee's thoughtful interest and leadership in blockchain technology and how it will help DHS accomplish its important mission. I look forward to your questions.

[The prepared statement of Dr. Maughan follows:]

Testimony of
Douglas Maughan
Division Director
Science and Technology
U.S. Department of Homeland Security
Before the
Committee on Science, Space, and Technology
Subcommittee on Oversight
Subcommittee on Research and Technology

May 8, 2018

Chairman Abraham, Chairwoman Comstock, Ranking Member Beyer, Ranking Member Lipinski and distinguished members of the Oversight and Research and Technology Subcommittees, thank you for inviting DHS to speak with you today. I will be addressing the topic of “Potential and proven applications of blockchain and distributed ledger technology in shipping, logistics, and customs, with an emphasis on supply chain management” and sharing with you important aspects of how we are exploring the use of blockchain and distributed ledger technologies in research and development and working with several DHS mission areas to integrate innovative technology into everyday use.

I have been in the Science and Technology Directorate (S&T) for 14.5 years working the entire time on Cybersecurity research and development (R&D). Prior to my time at DHS, I worked at the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency and have been involved in cybersecurity R&D as a government employee for over 30 years.

As the R&D arm of DHS, S&T develops the tools, technologies, and knowledge products for DHS operators, state and local first responders, and the nation’s critical infrastructure, ensuring R&D coordination across the Department to develop solutions for the needs of today and tomorrow. S&T partners with Federal agencies, industry, academia, and international governments to create and test solutions that help the nation’s homeland security officials prevent, respond to, and recover from all hazards and threats. S&T’s goal is to provide real-world solutions in a realistic timeframe.

The Benefits and Opportunities of Blockchains

Blockchains offer much promise, as can be seen in the rapid growth of interest across government and the private sector. From a government perspective, the technology holds the potential for enhanced transparency and auditing of public service operations, greater supply chain visibility to combat the distribution of counterfeit products, and automation of paper-based processes to improve delivery of services to organizations and citizens. Examples span the gamut from ensuring the authenticity and integrity of videos and photos from cameras, sensors and Internet of Things (IoT) devices; enhancing and facilitating international trade and customs

processes; facilitating and securing international passenger processing; to mitigating forgery and counterfeiting of official licenses and certificates.

Conversely, the challenge with blockchain technology is the potential for the development of “walled gardens” or closed technology platforms that do not support common standards for security, privacy, and data exchange. This would limit the growth and availability of a competitive marketplace of diverse, interoperable solutions for government and industry to draw upon to deliver cost effective and innovative services based on blockchain and distributed ledger technologies.

From the DHS S&T perspective, this is the trajectory we see for the blockchain and distributed ledger technologies in the near future:

- (A) Awareness of blockchain and its potential is increasingly becoming part of the mainstream business and government discussion. Fueled by promise, publicity, marketing, and market investment, organizations are looking for vendor-neutral guidance and best practices on when, where, why, and how this technology can be used. Such unbiased knowledge and implementation expertise is in very short supply, which will likely have significant impact on adoption.
- (B) The lack of best practices and implementation design patterns leads to knowledge and action asymmetries. In the race to achieve technological advantage and market share, decision criteria to evaluate the appropriate blockchain technologies are indeed appropriate for a particular situation are neglected. There are many types of blockchains with varying degrees of support of classic security principles such as confidentiality, integrity, and availability as well as support of privacy principles such as pseudonymity and selective disclosure. Analysis to determine if a particular blockchain supports these security and privacy considerations is either non-existent or not readily available.
- (C) There is an increasing tension between business/system owners, both in the private sector and public sector, and their technology and solution providers. For example, a technology provider’s desire to gain traction for their particular blockchain implementation may run up against the business/system owner’s expectation of having an open architecture environment for their systems, rather than vendor-specific approaches to prevent technology lock-in. Technology providers may recommend a replacement strategy to implement their blockchain, which runs counter to the business/system owners desire for new technology to integrate with their current business processes and technology to preserve and leverage existing investments.
- (D) Private industry is leading the way in blockchain development, as many see implementing blockchain as a key competitive advantage. The private sector’s significant investments and the ability to adopt technologies and processes faster than the public sector presents the government with a key decision point on how to best participate in this growing, but still nascent field. Government must be informed and ensure blockchain technology -- as it evolves -- supports standardized approaches for security, privacy, and data exchange to create efficiencies and enhance the public good. Government must also

consider leadership opportunities within the broader community and partner with industry to bring solutions to market.

DHS S&T and Blockchain

As the Science Advisor and the R&D arm of the Department, supporting the needs of our operational components is among our highest priorities. DHS S&T's decision approximately three years ago to start evaluating the security and privacy implications of blockchain technologies as well as our funding and involvement in the technical work since that time has resulted in placing our emphasis on architecture, standards, and interoperability and has allowed us to bring a level of rigor, expertise, and credibility that is unique in supporting DHS Components and other partners across the U.S. government.

Blockchain technologies are an integral part of several ongoing S&T research projects with DHS Components and other partners for a variety of purposes, including: developing best practices and decision criteria on when and how to implement blockchain technologies; understanding the support for security and privacy principles in commercial blockchain implementations; developing a decentralized identity broker that separates authentication and attestation services; learning about best practices for connecting legacy systems with blockchain enabled capabilities; developing specifications to ensure standardized approaches for decentralized identifiers; interoperable data formats using verifiable credentials and scalable and usable approaches to decentralized key management systems. These specifications, which are or will be submitted by S&T performers to global standards organizations to undergo an open, multi-stakeholder standardization process, are open, royalty-free, and free to implement, and are accompanied by implementation lessons to demonstrate their utility.

S&T Engaging CBP

Within DHS, U.S. Customs and Border Protection (CBP) has been the most active operational component to lean forward in partnering with S&T on exploring the use of blockchain and distributed ledger technologies for its mission. Our ongoing engagements with CBP include:

- Proof of concept deployments with the U.S. Border Patrol to evaluate how blockchain technology can be used to ensure the imagery and sensor data from cameras, fixed and mobile, can be ensured for authenticity and integrity.
- Conducting analysis of alternatives and blockchain technology feasibility explorations with the CBP and others to understand the potential benefits and challenges in using blockchain technology for enhancing and facilitating international passenger travel.
- Conducting proof of concepts deployments in partnership with CBP's Office of Trade and Office of Trade Relations that are directly focused on applications of blockchain and distributed ledger technology to shipping, logistics, and customs by providing visibility into globally distributed supply chains to help facilitate the movement of legitimate goods while combating the distribution of counterfeit goods.

A good example for a proof of concept effort with CBP on imagery and sensors involves the Internet of Things (IoT) Security. Based on CBP's technical requirements S&T engaged an Austin, Texas startup company, via the DHS Silicon Valley Innovation Program. This project captured and made clear the architecture choices and design decisions inherent in building an immutable record of data coming from cameras, sensors and IoT devices. It resulted in lessons

learned regarding the key issues that exist when integrating new technologies with existing government business and technical processes and the choices needed to ensure that private data should not be resident on a public blockchain while enabling the ability to publically validate the private data. S&T conducts its projects over multiple phases to minimize project and technical risk and this project is beginning deployment in an operational environment in partnership with CBP.

Blockchain Technology and Trade

DHS S&T, CBP Office of Trade (OT), and CBP Office of Trade Relations (OTR) are working together with private sector members of the Emerging Technologies Working Group of the CBP Commercial Customs Operations Advisory Committee (COAC) on multiple proof-of-concept implementations to identify the utility and feasibility of blockchain technology. DHS S&T conducted a two-day workshop with the COAC industry partners to provide information to the participants so that they are able to actively engage in the discussions about blockchain use with CBP. Included in the workshop was the development of a shared set of criteria to be used to evaluate the proof-of-concepts S&T and CBP (OT and OTR) would embark upon. Those criteria included:

- Use of an existing business process rather than creating something new.
- Ability to define metrics related to the existing business processes to ensure that the development of new technologies can be measured against existing metrics as a success criterion.
- Ability to run the blockchain enabled business process in parallel with existing business processes (A/B Testing).
- Needs to benefit a broad range of stakeholders.
- Must involve multiple roles and information sharing with differing parties who do not wish to have a shared infrastructure.
- Defined data model for data to be shared.
- Lessons learned to inform programs, requirements or regulations.

Using this criterion to walk through the various use cases of interest, resulted in a prioritized list of potential proof-of-concepts. We are currently executing the highest priority one which is to track free trade qualifications of imported goods by providing greater supply chain visibility, which would answer the following question, "Can distributed ledger technology be used to verify that an item qualifies for a free trade import tax exemption by demonstrating that the necessary percentage of an item's components were produced/assembled in a FTA country?" For this first Customs use-case, we are currently in the proof-of-concept phase with a Blacksburg, Virginia company. It is testing certificates associated with two particular Free Trade Agreements: the North American Free Trade Agreement (NAFTA) and the Central America Free Trade Agreement (CAFTA). Recently, S&T and CBP provided a 2-day exchange meeting into the technical requirements with the various trade and policy groups. The project has transitioned from the operational design phase to the technical requirements development and testing phase. There will be careful analysis of the success metrics at the end of this phase that will result in a GO/No-Go decision for the next phase.

Flexible Ledgers with Verifiable Credentials, Blacksburg, VA company

This project designed and implemented a generalized, configurable ledger technology that can support application specific needs while using a standardized, extensible core data model to ensure interoperability. It has resulted in a commercially available capability that incorporates interoperability specifications such as DIDs and Verifiable Credentials which are both on the standardization path via the World Wide Web Consortium (W3C). Given its support for these specifications, this technology is being used by the DHS/CBP Office of Trade in partnership with S&T for its first customs proof-of-concept.

Additional Blockchain Projects

In addition to work with DHS/CBP, S&T has contributed to the following efforts that have influenced and informed our supply chain focused blockchain work:

Decentralized Identifiers (DIDs), Seattle, WA company

Developed a decentralized identifier (DID) specification that enables the creation of a globally unique identifier without the need for a central registration authority. This identifier should be immutable, globally resolvable and cryptographically verifiable. At the end of this project a draft specification was developed and the Seattle, WA company was acquired by a Herriman, UT company.

Decentralized Key Management System (DKMS), Herriman, UT company

Using the DID specification developed by Respect Network Corporation, designed, developed and implemented a decentralized key management capability that is compatible with the requirements of the National Institute of Standards and Technology (NIST) 800-130 Cryptographic Key Management System Framework. Currently, the results of this work which includes the NIST 800-130 analysis as well as the architecture and design of the DKMS system is complete and has contributed to the open source Hyperledger Indy project (led by the Linux Foundation) for public review and comment. Next steps include a reference implementation as well as further test and evaluation based on community feedback.

Decentralized Identity Broker, Toronto, Canada company

This project designed, developed and implemented a decentralized identity broker that separates authentication and attestation services while ensuring resiliency against denial of service attacks, preventing honeypots of data, providing citizen centric consent and control of data sharing, while supporting international standards for identity assurance, privacy and data sharing. It has resulted in a commercially available capability that utilizes the Hyperledger Fabric project (also led by the Linux Foundation) that is currently undergoing operational testing in preparation for production deployment in the U.S. market.

A Path Forward

As noted before, a very real concern in the current timeframe of blockchain technologies is the potential for the development of “walled gardens” or closed technology platforms that do not support common standards for security, privacy, and data exchange. This would limit the growth

and availability of a competitive marketplace of diverse, interoperable solutions for government and industry to draw upon to deliver cost effective and innovative services based on blockchain and distributed ledger technologies.

To that end, DHS S&T is pursuing two broad courses of action to encourage a more open and inclusive future for blockchain technology:

1. Support development of globally available specifications (precursor to standards) that are open, royalty free, and free to implement to ensure interoperability across systems while ensuring there is no vendor lock-in.
 - a. Decentralized Identifiers (DIDs) via World Wide Web Consortium (W3C) Standardization Process
 - b. Verifiable Claims Data Model via W3C Standardization Process
 - c. Decentralized Key Management System via TBD (Potentially OASIS)
2. Actively work with and support our DHS Component customers, such as CBP, to understand their potential use cases for blockchain and help them achieve their outcomes with the needed R&D expertise and technologies.

We believe that our careful and considered approach benefits not just us but everyone who is considering the use of a blockchain technology in the long term by ensuring there is no vendor lock-in and there are multiple vendors with interoperable solutions from which we can buy.

Summary

Chairman Abraham, Chairwoman Comstock, Ranking Member Beyer, Ranking Member Lipinski, and distinguished members of the Oversight and Research and Technology Subcommittees, thank you again for your interest in blockchain or distributed ledger technologies and how these technologies will help DHS accomplish its important mission areas.

DHS S&T is focused on applied R&D of technologies with critical significance to DHS Components and other key parts of the Homeland Security Enterprise. Blockchain and distributed ledger technologies are rapidly moving from hype to reality in application domain areas where DHS S&T is currently working. This reality means DHS S&T must aggressively work with its research, development, test and evaluation partners throughout government and industry so homeland security applications of blockchain and distributed ledger technology are effective and trusted. This requirement includes strong working relationships with industry, so homeland security applications can leverage the best of industrial innovation, and homeland security capabilities can continue to support the strengthening and growth of American economic capabilities. These efforts must contribute to key challenge areas for all critical missions of DHS.

Thank you for your thoughtful leadership on these issues. I look forward to your questions.

APPENDIX: Selected References Blockchain and Distributed Ledger Technologies

Decentralized Identifier Primer, GitHub.com, October, 2017,
<https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/draft-documents/did-primer.md>.

A Verifiable Claims Primer, GitHub.com, October 2017,
<https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/draft-documents/verifiable-claims-primer.md>.

DKMS (Decentralized Key Management System) Design and Architecture V3, GitHub.com, April 12, 2018, <https://github.com/hyperledger/indy-sdk/blob/master/doc/dkms/DKMS%20Design%20and%20Architecture%20V3.md>.

NISTIR 8202 (DRAFT) - Blockchain Technology Overview,
<https://csrc.nist.gov/publications/detail/nistir/8202/draft>



**Homeland
Security**

Biography



W. Douglas Maughan, Ph.D.

Director, Cyber Security Division

Science and Technology Directorate

Dr. Douglas Maughan is the Division Director of the Cyber Security Division in the Homeland Security Advanced Research Projects Agency (HSARPA) within the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS). Dr. Maughan has been at DHS since October 2003 and is directing and managing the Cyber Security Research and Development activities and staff at DHS S&T. His research interests and related programs are in the areas of networking and information assurance. Dr.

Maughan has been responsible for helping bring to market over 40 commercial and open-source information security products during the past 12+ years while at DHS and is the Senior Executive responsible for the DHS Silicon Valley Innovation Program.

Prior to his appointment at DHS, Dr. Maughan was a Program Manager at the Defense Advanced Research Projects Agency (DARPA). Prior to his appointment at DARPA, Dr. Maughan worked for the National Security Agency (NSA) as a senior computer scientist and led several research teams performing network security research.

Dr. Maughan received Bachelor's Degrees in Computer Science and Applied Statistics from Utah State University, a Masters degree in Computer Science from Johns Hopkins University, and a PhD in Computer Science from the University of Maryland, Baltimore County (UMBC).

###

Chairman ABRAHAM. Thank you, Dr. Maughan.
I now recognize Mr. Chiaviello for five minutes to present his testimony.

**TESTIMONY OF MR. ROBERT CHIAVIELLO,
IPR COUNSEL, NUBY LAW**

Mr. CHIAVIELLO. Mr. Chairman, Members, thank you for focusing a light on this problem. I also want to thank your staff for helping to coordinate and the hospitality they've shown us coming up from Monroe, Louisiana, for this hearing.

I represent Luv N' Care. It's a company located in Monroe, Louisiana, and we make baby products. If you're a parent or grandparent of small children, you probably are familiar with our products. We make sippy cups, pacifiers, bibs, a wide range of products. We're not a tech company, so—but I'm here to explain to the Committee a problem—a growing problem that we are experiencing from unfair competition, particularly unfair competition from overseas.

As a consumer products company, we've always had to deal with people who would copy our intellectual property and try to sell it to—as counterfeits or knockoffs, but today, what we're facing is a foreign-centered threat. It's costing our company millions of dollars a year, and it's seriously affecting our bottom line.

Some of the—what we are seeing today is really a combination of two things. One is online retailing, combined with the ability to ship products directly from overseas into the U.S. market. When I first started 30-some years ago, if there was unfair competition, it usually came in by a container load, which usually gave us plenty of time to deal with it or—either on the water or by the time it arrived here we—we could deal with it either with customs or in the court system.

Today, the products are coming in by UPS and China post. What we see is a foreign-based entity that will use an online retailer like Amazon or others. They market their product to U.S.-based consumers. Typically, they use our intellectual property. They're using our trademarks to promote their product. They'll even go so far as to copy our photographs from our website, photograph our products, marketing it as their own. Then, they use digital advertising to attract the consumer to their website. The consumer thinks of course that the product is somehow related to us, purchases the product, and then the product is shipped directly to the consumer from, typically, China.

We are now—and this—the product can be shipped in. We've done experiments or testing. It can be 48, 72 hours from placing an order online to the time the product arrives here in the United States.

The—well, let me see. The—another—well, our problem is primarily with intellectual property where we can enforce our rights. There's also a problem with U.S. health and safety laws. Baby products are a fairly regulated item between the Consumer Products Safety Commission and the FDA, and our company spends a great deal of effort, resource complying with those rules and regulations, as well as our own quality standards.

Quite often, these pirates do not. We—some of the products that we've inspected, they use inferior materials. They use banned materials. The products don't comply with the size regulations of the CPSC. We've found pacifiers, for example, that are made using inferior plastic materials or with adulterants so that the nipple part can come off the pacifier, obviously can become a choking hazard.

And the U.S. consumer, as well as we, have no recourse. These folks are located—these pirates are located in China. They have no domestic connection, and our current systems for trying to enforce U.S. IP laws and health and safety regulations fail when the infringer or the violator is located overseas and outside the jurisdiction of U.S. courts and customs.

The way we see the problem, it's really a question of how the border is opened, and we implore for some solution to try and place better controls on the border to prevent these kinds of—this kind of activity.

I want to thank the Committee for its attention to this problem.
[The prepared statement of Mr. Chiaviello follows:]

**WRITTEN TESTIMONY OF ROBERT M. CHIAVIELLO, JR. ON
BEHALF OF LUV N' CARE, LTD. AND ADMAR
INTERNATIONAL, INC. TO THE U.S. HOUSE OF
REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE AND
TECHNOLOGY, SUBCOMMITTEE ON OVERSIGHT AND
SUBCOMMITTEE ON RESEARCH & TECHNOLOGY**

Executive Summary

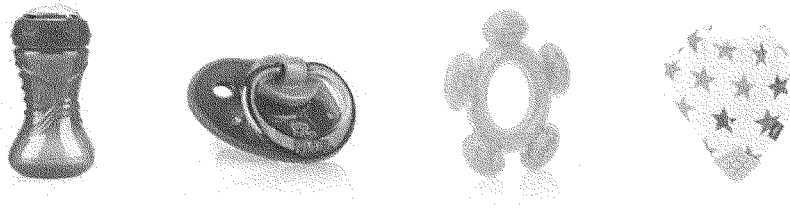
International unfair competition through the sale of counterfeit and pirated products has been dramatically increased by the combination of unrestricted online retailers and an open unregulated boarder that permits counterfeiters and pirates to directly ship to consumers in the US their counterfeit and pirated products. A growing concern involves sales of knock-off products from third party sellers who acquire and ship small quantity lots and individual packages from foreign locations to US consumers completely bypassing US laws and regulations relating to intellectual property, product health and safety requirement and without paying state and local taxes.

Luv n' care, Ltd. and Admar International, Inc.

Luv n' care, Ltd. (LNC) is a baby products company located in Monroe, Louisiana. LNC has been in business for more than forty years and in that time has excelled as a designer, manufacturer and seller of innovative, high quality and attractive products for babies and small children. LNC's products are sold under the NUBY brand and are among the most popular and well-known baby products in the industry. The NUBY brand and logo are famous throughout the United States

and worldwide. Based on its innovative, high quality and attractive designs, LNC is now known as one of the leading baby product companies in the United States and throughout the world. LNC protects the intellectual property in its innovative, high quality and attractive products through a combination of patents, trademarks and copyrights. Admar International, Inc. (Admar) owns and manages the intellectual property developed and used by LNC.

Representative examples of LNC's products are set out below:



Types of Unfair Competition

There are two forms of unfair competition affecting LNC. LNC faces unfair competition from the sale of knock-off or counterfeit products that are copies of or colorable imitations of LNC's products. While the knock-off products may visually resemble LNC's products they are often made using substantially inferior materials and workmanship and without regard to US health and safety regulations.

The counterfeiters then market their knock-off products directly to consumers by unlawfully using LNC's trademarks and copyrights in their online advertising. In many instances, the consumer is tricked into purchasing the knock-off product thinking it is the legitimate LNC product. As a result of these unlawful activities by the knock-off sellers LNC and Admar are losing millions of dollars in sales.

Another form of unfair competition relates to foreign competitors who do not comply with US health and safety regulations placing consumers at risk when they receive knock-off goods that are counterfeits of inferior quality and that do not comply with US health and safety laws and regulations. These unscrupulous sellers enjoy cost advantage in two respects. One, they use inferior less expensive materials of poor quality and two, they do not incur the expense of complying with US health and safety laws and regulations. LNC will inevitably have a higher cost structure as it uses high quality and relatively more expensive materials and bears the cost of complying with US health and safety laws and regulations. Consumers, regardless of how cost conscious they may be, will oftentimes select the less expensive product where they can discern no differences. This is

particularly problematic with online sales as the consumer cannot discern quality differences from photographs and this is especially true where the seller unlawfully expropriates a photograph from the original seller or brand owner.

The Knock-Off Products Industry

Counterfeiting and pirating popular branded products is an industry, primarily centered in China. As soon as a product is successful, Chinese manufacturers rush to copy the product or knock it off.¹ The knock-off manufacturers do not now typically copy the product identically but, in most instances, make small modifications, usually to cut corners on quality and make the product cheaper. The knock-off is almost always made of inferior poor-quality materials and regard for fit and finish is often ignored. The knock-off manufacturers will sometime offer their knock-off products directly to consumers but in most instances, they will sell directly to online sellers and small retailers via online marketplaces such as Alibaba. In addition to cutting costs by using inferior and less expensive inputs, the knock-off manufacturers also enjoy a cost advantage by not having to incur the expense of

¹ A knock-off is distinguished from a copy by exhibiting small variations from the original whereas the copy is identical. In either case it is hard for the untrained consumer to distinguish the original from the copy or knock-off.

complying with US health and safety laws and regulations. They also have a further cost advantage by not having to incur the research and development costs in creating a new product.

The next step in the knock-off industry distribution chain is the knock-off sellers who take advantage of the online marketplace offered by Amazon and eBay. These knock-off sellers create very low overhead online stores where they promote and sell their knock-off products directly to US consumers. The knock-off sellers are often physically located outside the US and most often in China. The knock-off seller offers the knock-off product directly to US consumers with no indication that the seller is located outside the US. Purchased knock-off products are then shipped directly to the US consumer via the foreign postal services, UPS or other carriers. In other cases, the knock-off seller will arrange to have the sales fulfilled by Amazon or other third parties. In the case of products fulfilled by Amazon, the seller will ship small quantities (less than container loads) to an Amazon fulfillment center. In almost every instance of a foreign knock-off seller, the seller uses a fake name, no contact information is provided, and the domain name

owner is hidden behind privacy settings. The knock-off products almost never include any indications of the manufacturer.

The sellers create online storefronts that often use brands in headlines and banners and embedded in the metadata or as key words. Some particularly flagrant knock-off sellers will even use photographs of the branded product and sometimes copy actual photographs of the product posted on the branded sellers website. The clear intent of these knock-off sellers is to create as close a look and feel as possible to the branded product, so the consumer is tricked into thinking that the knock-off seller is selling the branded product. Knock-off sellers also purchase ad words from Google and other search engines that include the brand name so that a consumer searching for the branded product will receive search results promoting the knock-off product. Without careful examination it is likely the consumer will be tricked into believing that the ad is sponsored by the brand owner creating a likelihood that the consumer will purchase the knock-off product instead of the branded product.

These problems are further exacerbated by the fact the knock-off sellers hide their identities and are often located outside the United

States. In a typical situation a knock-off seller will offer the knock-off products using a fictitious name with no identifying information. If notified of the infringement, the typical knock-off seller will remove the item or close the online store and reopen a new store under a different name selling the same products. LNC has been informed that Amazon alone has over 80,000 third party sellers making it almost impossible for a brand owner to comprehensively police that marketplace.

The knock-off manufacturers and sellers have inherent and substantial cost advantages verses the cost borne by the brand owners and can offer the knock-off product at a slightly lower price point. But because the knock-off manufacturers and sellers enjoy such a substantial cost advantage, they can reap enormous profits. So long as there is a substantial profit potential, the knock-off industry will continue to flourish.

Uncontrolled Exports to the US

Recently, LNC has observed a new sales model where knock-off sellers distribute products directly to US consumers in small quantities and oftentimes in individual packages. In the past, sellers would acquire products in large, typically container size, quantities. The

containers would be shipped to the US through conventional channels that were subject to US Customs and Border Control supervision. While it was a challenge to stop knock-off products at the border, it was possible if the manufacturer was known. Now, with the proliferation of online retail outlets, knock-off sellers, whether they are manufactures or re-sellers, can ship directly to US consumers from locations outside the US. LNC has observed knock-off shipments delivered via the national postal service, UPS and freight consolidators. The shipping companies do not provide detailed shipper information and the packaging typically does not include either a valid or direct return address. Generally, there is no indication on the packaging identifying the goods or the seller.

Online Retailers & Electronic Flea Markets

Online retailers such as Amazon have two selling models. In one model, the online retailers buy products from the manufacturers and resell those products online for their own accounts. In these instances, the online retailers are acting conventionally. In the second model, the online retailers acts as a service provider making available to third parties an online storefront where the third party seller can for the

most part sell whatever it wants. The service provider generally integrates third party sellers into its payment and delivery systems but claims it does not direct the activity of the seller or have any control over what is offered for sale. In this model, the service provider is acting like the owner of a digital flea market. It does not appear that the service providers exercise any supervision over who sets up the online storefront or whether those sellers comply with US laws and regulations and aside from blocking an offending storefront on occasion, no other remedial action is available.

Intellectual Property (IP) Infringement

The United States offers strong protection for patents, trademarks and copyrights. LNC takes advantage of all these forms of IP protection and has obtained numerous utility patents for its innovations both in the United States and throughout the world. LNC has also obtained design patents for its unique and attractive product designs. For its trademarks, LNC relies primarily on its common law rights but has registered its NUBY brand in the US and throughout the world. LNC also enjoys copyright protection for its graphical and sculptural works.

The knock-off products will typically violate LNC's patents and copyrights as well as its trade dress rights in its unique and popular product configurations. The knock-off sellers will also use LNC's trademarks in promoting and advertising the knock-off products. A particularly pernicious form of trademark infringement is the use of LNC trademarks in ad word purchases from search engine providers such as Google and Bing. In this situation, in response to a consumer performing an online search using an LNC product name, an advertisement is placed at the top of the search results with a link to the knock-off seller's online store. The ad typically makes it appear that the source of the product is the actual brand owner. If the consumer clicks on the ad, he or she is connected to the knock-off seller's online store or website where the consumer can purchase the knock-off item. In some instances, the knock-off seller will use copies of LNC photographs and other promotional materials, in direct violation of LNC's copyrights, in advertising the knock-off product.

Non-Compliance with US Health & Safety Regulations

The US Food & Drug Administration and the Consumer Products Safety Commission provide various regulations governing certain

aspects of the manufacture and sale of products directed at children and infants.² For example, products that are likely to be put into the mouth of a child or infant, such as pacifiers, must meet specific size requirements to avoid creating a choking hazard. LNC uses extreme care in the design and manufacture of its products to assure that they meet all applicable standards. LNC has seen products from third party sellers that do not meet these US health and safety requirements. While these products are typically not exact knock-offs of LNC products they still constitute unfair competition to the extent these third-party sellers do not incur the expense of compliance. LNC invests substantial resources in complying with health and safety regulations, an expense that must be recovered as part of the cost of the product. Non-compliant third-party sellers do not incur these costs and enjoy an inherent cost advantage over LNC. Not only is LNC being directly damaged by the sale of these non-compliant products, but they put US consumers – infants and children – at risk.

² Examples of regulations governing the design and manufacture of baby products include: 16 CFR 1500 (hazardous substances and articles), 16 CFR 1501 (small part), 16 CFR 1510 (rattle), 16 CFR 1511 (pacifier), mandatory toy standard ASTM F963, Battery Act, PL 104-142, 16 CFR 1303 (lead in surface coatings), 16 CFR 1307 (phthalates), 21 CFR 170 through 189 (food contact materials), 21 CFR 177.1580 (BPA-based PC resins), FDA Policy Guide section 500.450 (baby bottle nipple) and The Model Toxics in Packaging Legislation.

Choking Hazards

There are regulations governing the size of objects that are targeted for children and infants and especially for objects that will be chewed or put into the mouth. There are governing regulations that specify, for example, that pacifiers must meet minimum size requirements. It is also important that items such as nipples, pacifiers and teethingers be constructed of materials that are strong enough to resist separation in the mouth. If a nipple were to be detached from its base it could pose a serious choking hazard. LNC meets these regulations by carefully designing its products to meet these regulations and supervising its manufacturers to ensure that they comply with all US health and safety laws and regulations as well as LNC's strenuous quality controls. Knock-off manufacturers often use inferior plastics and add fillers to cut costs that weaken the materials. LNC has observed nipple separation in knock-off products that can pose serious choking hazards. To the extent foreign manufacturers and knock-off sellers attempt to modify LNC designs to avoid copying, they may not comply with the size regulations. LNC has observed undersized

pacifiers that could pose choking hazards. Where manufacturers and sellers can sell into the US marketplace with impunity, it encourages aggressive cost cutting and one of the first costs to be cut is compliance with health and safety regulations resulting in the distribution and sale of unsafe products to US consumers.

Strangulation Hazards

Another regulation relates to the size of loops for products such as lanyards and other items. An item to be used with a child or infant cannot have a loop that would fit over the head that might result in a strangulation hazard. This is especially problematic with adjustable loops that must have stops or other devices to prevent the loop from being too large. LNC has observed products with loops that are both too large and have ineffective stops.

Teether Regulations

Teethers are governed under the FDA as dental devices. The FDA regulations require that all manufacturing facilities used in the manufacture of dental devices be registered and approved by the FDA. LNC has invested substantial resources of time and money to qualify its manufacturing facilities. FDA regulations require that the approved

facility be listed on the packaging and that the manufacturer be listed on an FDA database. LNC has observed teether products that do not identify an authorized manufacturing facility on the packaging and do not have any manufacturing facilities listed on the FDA database leading it to believe these products were made in unapproved facilities. These unscrupulous manufacturers and sellers are distributing and selling potentially unsafe products to US consumers.

Outlawed Materials

Various federal and state regulators have identified certain materials that they deem to be potentially harmful and should not be used in the manufacture of baby products. LNC designs and specifies that its products must be free of these materials and invests substantial resources in supervising its manufacturers and testing their products to ensure that no harmful materials are ever used in LNC products. LNC has observed that many knock-off manufacturers and sellers are distributing and selling products that include one or more of these banned substances. In many instances, the packaging claims that the product is free of these materials. In those cases, not only are potentially

harmful products being distributed and sold to US consumer, but they are also being lied to in false advertising and promotion.

Inadequate Judicial Remedies

Foreign manufactures and sellers take advantage of US judicial procedures and treaties to avoid prosecution in US Courts. One strategy employed by the knock-off sellers is to obfuscate and hide behind false or anonymous identities. In order to bring a direct action in US courts, there must be personal jurisdiction over the defendant. Personal jurisdiction is obtained by serving a summons and complaint on the named defendant or its agent for service of process. To serve the summons and complaint, a physical address is needed. Many, if not most, online sellers use identities that are unrelated to the real party in interest. In almost every case, the online seller does not provide a physical address or contact information. When the sellers identity is actually revealed, it is often an address in a remote part of China that upon further investigation turns out to be false. Even when an identity is revealed, and a true address located, US plaintiffs are required to serve Chinese entities under the Hague Convention. Under normal circumstances service of process under the Hague Convention in China

takes on the order of nine months. Since 2015, China has refused to complete the service of process requested by US Courts leaving US plaintiffs with any ability to serve Chinese defendants. Without complete service there is no personal jurisdiction and the US court cannot act. In the event service on the foreign defendant is completed and the defendant fails to appear, the plaintiff brand owner can obtain a default judgment that may be used to remove the knock-off defendant from an online store hosted by an online service provider. Even if the US plaintiff employs alternative service by Court order and obtains a default judgment, China refuses to honor those judgments leaving the US plaintiff with no direct remedy against the violator.

As explained below, blocking a specific knock-off online seller does not solve the problem as the knock-off seller simply continues selling the knock-off products under another name in a different online store. As the entire process of filing the complaint, completing service of process and seeking a default judgment can take upwards of a year, the plaintiff brand owner is forced to suffer additional damages with little to no likelihood of ever receiving compensation.

Inadequate Customs & Border Patrol Remedies

The US Customs & Border Patrol appear to be unprepared for dealing with a distribution model that relies on small package shipments into the US. It has always been difficult to stop shipments at the border due to the many ports of entry and the volume of shipments into the US. Typically, US Customs requires the rights owner to identify the port of entry and the vessel carrying the knock-off products. Since most of the knock-off manufacturers do one-off products or small runs, by the time the brand owner learns of the knock-off the goods are already in the US. When shipments are in smaller quantities or in individual packages, it is almost impossible for the US Customs authorities to interdict the knock-off packages. This problem is further exacerbated by the fact the actual seller/shipper is unknown to the brand owner. These inadequacies in the judicial and customs systems leave the only remedy with some private action against the service provider for the online seller.

Online Takedowns are Not the Solution

While the online service providers do provide some relief for rights owners, that relief is very limited and does not address violations

of US health and safety regulations. First, online service providers will only grant relief to rights owners that have federally registered trademarks and copyrights.³ Second, no relief is provided to common law trademark owners. Third, the takedown process is automated and subject to the vagaries of technology. While online retailers do provide procedures for escalating takedown requests, that escalation procedure adds delay and a degree of subjectivity to the process. And to the extent that relief is provided it is merely limited to blocking the online seller. Even if the knock-off seller is blocked, there is no mechanism in place to prevent that seller from setting up a new online store with a different name selling the same knock-off goods. Finally, takedown procedures are not designed to address violations of health and safety regulations. Direct action against the online service provider is difficult as US law requires notice and cases have held that the service provider is not liable for the actions of independent third parties.

Conclusion

International unfair competition through the sale of counterfeit and pirated products has been dramatically increased by the

³ While technically a patent owner can use the takedown process, in most cases the online retailer is not willing to go through the process of confirming infringement absent a court order or judgment of infringement.

combination of unrestricted online retailers and an open unregulated boarder that permits counterfeiters and pirates to directly ship to consumers in the US their counterfeit and pirated products. A growing concern involves sales of knock-off products from third party sellers who acquire and ship small quantity lots and individual packages from foreign locations to US consumers completely bypassing US laws and regulations relating to intellectual property, product health and safety requirements and without paying state and local taxes.

Respectfully submitted this 7th day of May 2018.

By: /s/ Robert M. Chiaviello, Jr.
 Robert M. Chiaviello, Jr.
 Louisiana State Bar No. 37370
 New York Bar No.
 Texas Bar No.
 DC Bar No.
 E-Mail: bobc@nuby.com
LUV N' CARE, LTD.
 3030 Aurora Avenue
 Monroe, LA 71201
 Tel No.: (318) 338-3603
 Fax No.: (318) 388-5892

*Counsel for Plaintiffs, Luv n' care, Ltd.
 and Admar International, Inc.*



Monroe, LA
(318) 410-4012
bobe@nuby.com

Biography

Robert M. Chiaviello, Jr. Attorney and Counselor-at-Law

Bob Chiaviello has been practicing intellectual property law for over 37 years. Bob grew up in Rutherford, New Jersey. After obtaining an undergraduate degree in physics from Washington & Lee University in Lexington, Virginia in 1977, Bob went to The John Marshall Law School in Chicago, Illinois. After graduating from John Marshall in 1980, Bob joined intellectual property boutique Pennie & Edmonds in New York City as an associate. At Pennie & Edmonds, Bob worked extensively on a wide range of litigation matters including cases involving the original patents for the hand-held calculator, point of sale terminals and the algorithm for providing lottery ticket security. From Pennie & Edmonds, Bob joined IBM in Charlotte, North Carolina where he was responsible for handling the intellectual property matters for the company's small printer division.

In 1989, Bob returned to private practice joining the firm of Baker, Mills & Glast in Dallas, Texas. A year later, in 1990, Bob joined Baker Botts' Dallas office. At Baker Botts, Bob was a partner in the IP group and worked on a variety of complex civil matters including cases in the fields of electronics, both hardware and software, and in the telecommunications, semiconductor, computer and power industry. In 2002, Bob joined the Dallas office of Fulbright & Jaworski as a partner and continued his litigation practice. In 2011 Bob retired from Fulbright to pursue other interests. He continued to represent clients in various licensing matters while also pursuing other business interests including a furniture making and restoration business. In 2015, Bob sold the furniture business and returned to the full-time practice of law when he joined the Luv n' care team as its IPR counsel.

Over the course of his 37-year career, Bob has personally handled hundreds of civil cases, including cases involving complex intellectual property and contract matters with numerous parties in multiple district courts. Bob has also maintained an extensive office practice including negotiating and drafting complex agreements, managing corporate compliance, as well as intellectual property procurement, including the preparation and prosecution of domestic and foreign patent, trademark and copyright applications, reissue and reexamination cases, Inter Partes Reviews, appeals and interferences, and the preparation of patent, copyright and trademark licenses.

Chairman ABRAHAM. Thank you, Mr. Chiaviello.
Mr. White, five minutes please, sir.

**TESTIMONY OF MR. MICHAEL WHITE,
HEAD OF GLOBAL TRADE DIGITIZATION, MAERSK**

Mr. WHITE. Good morning, Chairman Abraham, Chairwoman Comstock, Ranking Member Beyer, Ranking Member Lipinski, and members of the subcommittees. My name is Mike White. I'm head of Global Trade Digitization for Maersk. Before moving to my current role, I was President of Maersk Line North America for the past eight years, and I have had the pleasure of working in this industry for over 37 years. Thank you very much for the opportunity to testify this morning.

In a global economy, supply chains are of critical importance. It is estimated that over \$16 trillion worth of goods cross international borders each year, and more than 80 percent of those goods are carried by the ocean shipping industry. Over the past five years, global container volumes have increased on average of 3.7 percent per year.

Moving goods from point A to point B involves many parties who are separate but dependent upon one another. Importers and exporters, freight forwarders, customs brokers, ports and terminals, ocean carriers, customs and government authorities, inland transportation providers, financial institutions, and others all gather discrete sets of sometimes overlapping information, which they share using a convoluted web of individualized formats and aging technologies. This inconsistent flow of information across organizational boundaries hampers the efficient flow of goods, but through a collective complexity-driven inertia, supply chain participants persist in their outdated practices. Perhaps this is because they trust that, flawed though it may be, the system will deliver ultimately a container from point A to point B, and they can't afford to experiment with a system that may fail to do so.

The industry operates today much as it does—or has since the introduction of shipping containers in the 1950s. Many processes are manual, time-consuming, and too often paper-based, with transactions still frequently coming today via fax machine. The cargo on any given container vessel voyage generates a mountain of documents, many of which are sent to the relevant container's destination by some other means. Container shipments can often be delayed in the port because necessary paperwork has not caught up with the goods that they carry.

In a Freightos survey recently cited by The Economist, 2/3 of respondents said that over 1/4 of their deliveries abroad arrived late. Nearly 1/2 said they spend more than 2 hours on paperwork when arranging a given shipment, and the vast majority of respondents had real difficulty tracking goods in transit.

In an industry where global transport costs are 1.8 to \$2 trillion annually, administrative costs can sometimes exceed the end-to-end transport costs for a given container, and overall inefficiencies are estimated at 15 percent or higher. The World Economic Forum estimates that by reducing barriers within international supply chains, global trade could increase by up to 15 percent, boosting economy and creating jobs.

These barriers have proven incredibly difficult to surmount as participants are trapped by the layered complexity of entrenched methods. Everyone agrees that there must be a better way, but no single participant is able to affect change because of the overarching desire to stick with what is known to work even if not very well over an experiment that could fail with disastrous and cascading consequences.

In 2016, Maersk and IBM began a collaboration with the goal of digitizing the global supply chain. To begin, we analyzed a number of supply chains to understand the current challenges in specific areas of complexity. One of these involved a shipment of avocados moving from Kenya to the Netherlands. This one container involved over 30 different actors or entities, more than 100 individuals, and over 200 separate exchanges of information and documentation, the vast majority of which were completely manual, paper-based, and extremely time-consuming.

We soon realized that no sustainable solution can exist for streamlining this entrenched complexity without unprecedented buy-in from the entire industry. In our analysis, an open and neutral industry platform, consisting at its core of a worldwide network of interconnected supply chain participants, is by far the best way to drive efficient, transparent, and secure global trade. The trust necessary to build this network would likely not exist without blockchain technology.

In January of this year, Maersk and IBM announced our intention, subject to the receipt of all applicable regulatory approvals, to form a joint venture to implement this global platform. The platform will follow the flow of cargo from source to destination. As empty containers are provisioned and transported from a warehouse, as the containers are stuffed and transported to a port, loaded on board a vessel, cleared export regulatory clearance, and continuing on the vessel to the import side will follow the flow of the cargo through customs clearance and ultimately delivery to the final consignee and the empty containers returned to a depot.

The platform will do this by leveraging network participants who both make information available and consume information by others. Blockchain enables this unprecedented collaboration by ensuring the security, trustworthiness, and permissioned accessibility of sensitive participation information, even as that information is distributed across heretofore segregated enterprises. Participants will be able to go to one place to track the real-time status of a container and to locate and transact with up-to-date, trustworthy trade information.

Blockchain is the critical ingredient. It creates an immutable record of transactions, which enables the ecosystem to track the exchange of critical information like records of inspection, bills of lading, customs documents. Throughout the trade, each participant has real-time visibility access to supply chain according to permission levels. Trust is built by validating the participants, authenticating transactions, distributing information, and maintaining unalterable records that are located or accessible through the platform.

At the end of the given shipment, these immutable records will provide one version of the truth of how a container transited from

beginning to end, and the documents submitted to the platform can be actioned and stored using blockchain technology. This means that, once a document has been certified by a government agency, the slightest alteration to that document will be exposed and rejected as different from the original. This will obviously have lasting benefits towards fraud detection and prevention.

The result: a previously unattainable information backbone of the global supply chain, encompassing the milestones documents in a structured form, customs filings, and many more solutions. Access to this platform will give traders and transportation real-time end-to-end visibility of, and permission to access to, information about cargo shipments such as status and whereabouts of containers, shipping milestones, and trade documentation. As the network grows, its benefits will multiply and it will generate billions of dollars in savings for all industry participants, along with entirely new approaches to global logistics.

Thank you for the opportunity to discuss this vital topic. I look forward to answering your questions.

[The prepared statement of Mr. White follows:]

Mike White

Maersk Line A/S

Head of Global Trade Digitization

House Committee on Science, Space and Technology

Subcommittee on Oversight & Subcommittee Research and Technology

“Leveraging Blockchain Technology to Improve Supply Chain management and Combat Counterfeit Goods”

May 8, 2018

Introduction

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

My name is Mike White, and I’m the Head of Global Trade Digitization at Maersk. Before moving to my current role, I was the President of Maersk Line North America for the past eight years, and I have had the pleasure of working in this industry for the past 37 years. Thank you very much for the opportunity to testify this morning.

In a global economy, supply chains are of critical importance. It is estimated that over \$16 trillion worth of goods cross international borders each year and more than 80% of those goods are carried by the ocean shipping industry. Over the past 5 years global container volumes have increased on average by 3.7% per year.

Moving goods from point A to point B involves many parties who are separate from but dependent on one another. Importers and exporters, freight forwarders, customs brokers, ports and terminals, ocean carriers, customs and government authorities, inland transportation providers, financial institutions and others all gather discrete sets of overlapping information which they share using a convoluted web of individualized formats and aging technologies.

This inconsistent flow of information across organizational boundaries hampers the efficient flow of goods, but through a collective, complexity driven inertia, supply chain participants persist in their outdated practices. Perhaps this is because they trust that, as flawed as it may be, the system will deliver a container from point a to point b and they can’t afford to experiment with a system that may fail to do so.

The industry operates today much as it did at the introduction of shipping containers in the 1950s. Many processes are manual, time-consuming and too often paper-based (with transactions still frequently

occurring via fax machine). The cargo on any given container vessel voyage generates a mountain of documents—many of which are sent to the relevant container's destination by some other means. Container shipments can often be delayed in port because necessary paperwork has not caught up with the goods that they carry.

In a Freightos survey recently cited by the Economist 2/3 of respondents said that over ¼ of their deliveries from abroad arrive late. Nearly half said that they spend more than 2 hours on paperwork when arranging a given shipment and the vast majority of respondents had real difficulty tracking goods in transit.

In an industry where Global transport costs are 1.8 to 2 trillion dollars annually, administrative costs can sometimes exceed the end to end transport costs for a given container, and overall inefficiencies are estimated at 15% or higher. The World Economic Forum estimates that by reducing barriers within international supply chains, global trade could increase by up to 15%, boosting economies and creating jobs.

These barriers have proven incredibly difficult to surmount as participants are trapped by the layered complexity of entrenched methods. Everyone agrees that there must be a better way, but no single participant is able to effect change because of an overarching desire to stick with what is known to work (if not very well) over an experiment that could fail with disastrous and cascading consequences.

In 2016, Maersk and IBM began a collaboration with the goal of digitizing the global supply chain. To begin, we analyzed a number of supply chains to understand the current challenges and specific areas of complexity. One of these involved a shipment of avocados moving from Kenya to the Netherlands. This one container involved over 30 different actors or entities, more than 100 individuals and over 200 separate exchanges of information and documentation - the vast majority of which was completely manual, paper based, and extremely time consuming.

We soon realized that no sustainable solution can exist for streamlining this entrenched complexity without unprecedented buy in from the entire industry. In our analysis, an open and neutral industry platform, consisting at its core of a worldwide network of interconnected supply chain participants, is by far the best way to drive efficient, transparent, and secure global trade. The trust necessary to build this network would likely not exist without Blockchain technology.

In January of this year Maersk and IBM announced their intention, subject to the receipt of all applicable regulatory approvals, to form a joint venture to implement this global platform. The platform will follow the flow of cargo from source to destination: as empty containers are provisioned and transported to a warehouse, as the containers are stuffed and transported to a port, as the cargo undergoes regulatory clearance and is loaded onto an ocean carrier, and as the cargo is shipped across the ocean. Continuing on the import side, the platform will follow the flow of the cargo as it is cleared by applicable governmental authorities and transported to the consignee and empty containers returned to a depot.

The platform will do this by leveraging the network of ecosystem participants who both make information available to others and consume information made available by others, a virtuous cycle that will benefit everyone. Blockchain enables this unprecedented collaboration by ensuring the security, trustworthiness, and permissioned accessibility of sensitive participant information even as that information is distributed across heretofore segregated enterprises. Participants will be able to go to

one place to track the real-time status of a container and to locate and transact with up to date, trustworthy trade documentation.

Blockchain is the critical ingredient. Blockchain creates an immutable record of transactions, which enables the ecosystem to track the exchange of critical information – like records of inspection, bills of lading, and customs documents. Throughout a trade, each participant has real-time visibility across the supply chain according to permission levels. Trust is built by validating the participants, authenticating transactions, distributing information, and maintaining unalterable records that are located on or accessible through the platform.

At the end of a given shipment, these immutable records will provide one version of the truth as to how a container transited from beginning to end of its journey. Furthermore, documents submitted to the platform could be actioned and stored using blockchain technology. This means that, once a document has been certified by a government agency, the slightest alteration to that document will be exposed and rejected as different from the original. This will obviously have lasting benefits towards fraud detection and prevention.

The result: a previously unattainable information backbone of the global supply chain encompassing shipping milestones, documents in structured and unstructured form, customs filings, internet of things data, and much more. With access to that information, and the ability to utilize Blockchain to securely and confidently collaborate, the industry is poised to finally realize the enormous potential offered by true supply chain digitization.

Access to this platform will give traders and transportation and logistics providers real-time, end-to-end visibility of, and permissioned access to, information about cargo shipments such as the status and whereabouts of containers, shipping milestones, and trade documentation. As the network grows, its benefits will multiply and it will generate billions of dollars in savings for the industry along with entirely new approaches to global logistics.

Thank you for the opportunity to discuss this vital topic. I look forward to answering your questions and further exploring this topic.

Michael J. White

Head of Global Trade Digitization

A.P. Møller – Maersk

(Future CEO of Maersk and IBM's New Joint Venture)



Mike White manages the Global Trade Digitization organization for Maersk. He is responsible for a global team which aims to establish a global platform to facilitate trade and create more transparency, efficiency and security within supply chains. GTD is a major step in our commitment to solve the problems our customers face in getting real-time visibility in their supply chain and the lack of standards of moving goods internationally.

Mike White built his career at Maersk and prior at P&O Nedlloyd, joining the organization in 1990 before the company was acquired by Maersk in 2005. For nearly two decades, he has held a number of leadership roles across many geographies. Prior to his current role, he served for 8 years as President of Maersk Line's liner business in North America. Prior to this, he was Chief Executive for Maersk Line Central Europe managing activities for 12 countries. Before that, he was responsible for Maersk Logistics, Damco, Maersk Customs Services Inc, The Gilbert Company and Bridge Terminal Transport. From 1990-2005, Mike held a number of senior management positions including President & CEO of P&O Nedlloyd North America, President of Farrell Lines, and Director and Chairman of Port Newark Container Terminal.

He graduated from Virginia Wesleyan College in 1981, and has attended several executive programs at Harvard Business School and IMD Business School in Switzerland.

Mike is a licensed Customhouse Broker. He is a member of the Board of Trustees for Virginia Wesleyan University.

Mike lives in New Jersey, United States, with his wife and two children.

A.P. Moller Maersk highlights:

A.P. Moller Maersk is the world's largest global integrator of container logistics, using digital innovation in order to provide seamless and transparent solutions to customer's shipping and logistics needs.

Maersk Line Highlights:

- Global operation covers all major trade routes making 51,000 port calls in 378 ports p.a. in 121 countries
- 646 vessels with a capacity of 3.5 million TEU shipping 13.2 million containers (2016) serving 59,000 customers worldwide
- 29,900 dedicated employees including 7,800 seafarers.

About the Global Trade Digitization

The GTD will be an open platform which will allow the whole industry to share information in a secure way and thereby build more efficient and transparent processes and business models. Paper-borne processes as we know them today are costly and error-prone. In a nutshell, the overall benefits include a reduction in costs associated with the paper-trail between trading partners while streamlining the process of trade and making a more secure way to submit and approve documents across organizational boundaries.

You may can read more [about this solution here](#).



Chairman ABRAHAM. Thank you, Mr. White.
Mr. Rubio?

**TESTIMONY OF MR. CHRIS RUBIO,
VP GLOBAL CUSTOMS BROKERAGE STAFF, UPS**

Mr. RUBIO. Chairman Abraham, Chairman Comstock, Ranking Member Beyer—

Chairman ABRAHAM. Turn your mic on.

Mr. RUBIO. Thank you, sir. Chairman Abraham, Chairman Comstock, Ranking Member Beyer, Ranking Member Lipinski, and distinguished members of the committee, thank you for the opportunity to testify before you today on how blockchain technology can be leveraged to provide greater supply chain visibility and possibly help combat the distribution of counterfeit products.

I applaud the Committee's efforts to get in front of this rapidly evolving technology, and this hearing before two subcommittees speaks to the importance of this issue.

With over 434,000 global employees delivering more than 19 million packages and documents every day in over 220 countries and territories around the world, we work hard to be united problem solvers. At UPS, our business processes are complex and our technology advanced, but our objective is simple: to ensure world-class service for our customers.

UPS has been researching the use of blockchain technology with the purpose of identifying ways blockchain may impact, disrupt, and/or drive efficiency in the supply chain. Our goal is to engage in a collaborative discussion with customers and policymakers on how blockchain technology can be utilized to further enable supply chain digitization, efficiency, and security, blockchain as an enabler.

In terms of logistics applications, blockchain could bring together buyers, sellers, suppliers, payment companies, and logistic companies to provide end-to-end supply chain visibility, while addressing privacy and data security concerns. For government border agencies, blockchain could enable greater transparency of a transaction, possibly including what's in the box and who's buying it, how much they're paying for it, assurance that the duties and taxes are paid, and possible confirmation that shipments are not under-declared, resulting in faster release and a more trustworthy supply chain.

As a result of the technology underlying blockchains, UPS sees four key benefits for our company and our customers: integrity, transparency, interoperability, and security. In particular, our large customers have the potential to benefit greatly from the adoption of this technology.

Given the complexities of the modern supply chain, multinational corporations have invested large amounts of money in enterprise resource planning systems and supply chain management software yet only have limited visibility and insight into where all of these products are at a given point in time.

However, it is not only large multinationals that will benefit. We also see the potential for small and medium-size enterprises to realize the many benefits of blockchain, for example, a small business would be able to ship its products globally due to the blockchain

framework that enables multiple parties to share important trade information in a single ledger for the contents of that shipment.

As a protector of intellectual property rights, UPS and other express delivery service providers engage regularly with customers and governments to ensure that our network around the world only carries legitimate and legal products. However, there are practical limits to what we and other express delivery providers can do day-to-day. First, we're not the originators of the information about the shipments, and limitations exist on the quantity of information that we can obtain from customers. Second, we and other express delivery providers do not have the requisite expertise to identify counterfeit or pirated goods. And third, we're not law enforcement agencies, which means we're subject to national data protection and commercial information and confidentiality rules.

This is where blockchain could potentially provide a solution. By having the ability to track any product from the beginning of its journey through the supply chain, blockchain may provide a solution to unknown or unverified product origins. In fact, we are already seeing this technology used to trace the origins of various products from diamonds and mangos. By creating a digital record of each individual item, the company and consumer are able to verify the authenticity of the product and ensure standards are met each step of the way.

The United States and international governments' role in fostering blockchain: The U.S. Congress, federal agencies, and our international counterparts will play a vital role in the adoption and success of blockchain in the supply chain. Governments must take a balanced and measured approach between regulating this everchanging technology and allowing for its innovation and evolution. As e-commerce and global trade flows continue to rapidly grow, the United States must work with our international trading partners to establish a common set of blockchain standards that are recognized throughout the world.

As I mentioned previously, UPS operates in over 220 countries and territories around the world, and I know firsthand that a patchwork of global regulation would stifle innovation, slow the flow of goods across borders, and increase the likelihood that illicit material would enter the country undetected.

Despite the potential upside to the widespread adoption of blockchain, a couple of key barriers exist that must be overcome. The first and biggest hurdle is the linking of all physical objects to the digital stream. Currently, individual items may be tagged digitally with RFID, near-field communication, or two-dimensional barcodes. However, in order for blockchain to realize its full potential, all products would have to be tagged digitally, requiring an overhaul in today's supply chain practices. Without an industry and supply-chain-wide commitment to adopt to digitalization, many organizations will not make the investment in the technology.

Finally, the international community must come together to ensure that there is one unified set of standards for blockchain. This will give companies the confidence they need to know the technology they adopt will be recognized throughout the world. Without these common standards, uncertainty will prevent the largescale

investment that is needed to make blockchain a success in the supply chain.

Thank you once again for inviting me to testify before you on the technology that could change how the world understands supply chains. I look forward to any questions.

[The prepared statement of Mr. Rubio follows:]

**Testimony of Christopher Rubio
Vice President, Global Customs and Brokerage Staff
United Parcel Service**

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

Tuesday, May 8, 2018

Introduction

Chairman Abraham, Chairwoman Comstock, Ranking Member Beyer, Ranking Member Lipinski and distinguished members of the Committee, thank you for the opportunity to testify before you today on how blockchain technology can be leveraged to provide greater supply chain visibility and possibly help combat the distribution of counterfeit products. I applaud the Committee's efforts to get in front of this rapidly evolving technology, and this hearing before two subcommittees speaks to the importance of this issue.

With over 434,000 global employees delivering more than 19 million packages and documents every day in over 220 countries and territories around the world, we work hard to be United Problem Solvers. At UPS, our business processes are complex and our technology advanced, but our objective is simple: to ensure world-class service for our customers.

UPS has been researching the use of blockchain technology with the purpose of identifying ways blockchain may impact, disrupt and/or drive efficiency in the supply chain. Our goal is to engage in a collaborative discussion with customers and policymakers on how blockchain technology can be utilized to further enable supply chain digitization, efficiency and security.

Blockchain as an Enabler

A blockchain can be thought of as a distributed "database" of information and records created chronologically in a series of "blocks"—with each block having a timestamp and a connection to its previous block. The information contained in a blockchain, a cloud-based "ledger," is not stored in a single location; rather, it is shared and continually updated over a network of computers. One common example that some of us might use is that of a Google Doc: one can access a single, shared document from many computers, see edits from various people in real time, and any additions to the text are recorded and timestamped.

In terms of logistics applications, blockchain could bring together buyers, sellers, suppliers, payment companies and logistics companies to provide end-to-end supply chain visibility while addressing privacy and data security concerns. For government border agencies, blockchain could enable greater transparency of a transaction, possibly including what's in the box and who's buying it, how much they are paying for it, assurance that duties and taxes are paid, and possible confirmation that shipments are not under-declared—resulting in faster release and a more trustworthy product supply chain. To this end, we can envision a possible fast-path customs clearance procedure for validated/secured/authenticated shipments versus those that are not.

As a result of the technology underlying blockchains, UPS sees four key benefits for our company and our customers. First is integrity. Because a blockchain is spread among many different internet users, it cannot be controlled by any single party. Additionally, network failure—either intentional or unintentional—can't significantly disrupt it. Second is transparency. The information encoded in the

blockchain is accessible across the entire network because blockchain operates by mass collaboration and verification. Third is incorruptibility. Blockchain uses the latest encryption technology, and as a result, the ability to verify one's identity and the source of documents and products raises the level of trust in commercial interactions. Finally, blockchain provides a vitally important level of security. Anti-money laundering (AML) and know-your-customer (KYC) practices have a strong potential for being adapted to the blockchain. Currently, financial institutions must perform a labor-intensive, multi-step process for each new customer. These manual steps today can result in delays in the supply chain, resulting in products not getting to their ultimate destination in a timely manner.

In particular, our large customers have the potential to benefit greatly from the adoption of this technology. Given the complexities of the modern supply chain, multinational corporations have invested large amounts of money in enterprise resource planning (ERP) and supply chain management software yet only have limited visibility and insight into where all their products are at any given moment. Through the utilization of blockchain technology, companies' supply chain networks are able to create one overarching database without it having to be stored on one server or on one network. This will not only make these companies more efficient but also leave them better equipped to handle the continued growth of e-commerce.

However, it is not only large multinationals that will benefit. We also see the potential for small and medium size enterprises (SMEs) to realize the many benefits of blockchain. For example, by taking advantage of this technology, a small business will be more easily able to ship its products globally due to the blockchain framework that enables multiple parties to share important trade information in a single ledger for the contents of that shipment. By streamlining customs and duty procedures, the global marketplace will be more accessible and less intimidating for SMEs, allowing them to ship their products to new markets and drive growth by taking advantage of the massive buying potential of overseas consumers.

Blockchain as a Protector of Intellectual Property Rights (IPR)

Restricting the access of illicit and IPR-violating goods within networks is a top priority for many companies in our industry, especially given the need to ensure efficient, cost-effective and secure global supply chains. Every day, express delivery service (EDS) providers carry approximately 30 million shipments and, despite ongoing efforts, illegal goods make it into the system. In fact, in 2016, 63,000 IPR infringement cases were reported by EU Customs Authorities. Of these cases 8.3% involved express shipments but the vast majority of these cases (65%) involved postal shipments. Though the problem may be bigger in the postal lanes, it remains an active issue for EDS companies as well given that we are currently held to a higher standard than the posts.¹

UPS and other EDS providers engage regularly with customers and governments to ensure that our network around the world only carries legitimate and legal products. However, there are practical limits to what we and other EDS providers can do day-to-day: first, we are not the originators of information about shipments, and limitations exist on the quantity of information that we can obtain from customers; second, we and other EDS providers do not have the requisite expertise to identify counterfeit or pirated goods; and, third, we are not law enforcement agencies, which means we are subject to national data protection and commercial information confidentiality rules. These limitations underscore the importance of information sharing and collaboration between all involved parties—the rights-holders, customs authorities, and the EDS industry for preventing illicit and counterfeit goods from entering our system.

¹https://ec.europa.eu/taxation_customs/sites/taxation/files/report_on_eu_customs_enforcement_of_ipr_at_the_border_2017.pdf

This is where blockchain can potentially provide a solution. According to a recent Deloitte study, “blockchain could help companies understand how ingredients and finished goods are passed through each subcontractor, and reduce profit losses from counterfeit and gray market trading, as well as increase confidence for end-market users by reducing or eliminating the impact of counterfeit products.”² By having the ability to track any product from the beginning of its journey through the supply chain, blockchain may provide a solution to unknown or unverified product origins. In fact, we are already seeing this technology used to trace the origins of various products – from diamonds and mangos. By creating a digital record of each individual item, the company and consumer are able to verify the authenticity of the product and ensure standards are met each step of the way.

The U.S. and International Governments Role in Fostering Blockchain

The United States Congress, federal agencies and our international counterparts will play a vital role in the adoption and success of blockchain in the supply chain. Governments must take a balanced and measured approach between regulating this ever-changing technology and allowing for its innovation and evolution. As e-commerce and global trade flows continue to rapidly grow, the United States must work with our international trading partners to establish a common set of blockchain standards that are recognized throughout the world. As I mentioned previously, UPS operates in over 220 countries and territories around the world and I know firsthand that a patchwork of global regulation would stifle innovation, slow the flow of goods across borders and increase the likelihood that illicit material would enter the country undetected.

Increasingly, efficient border clearance is contingent on trust and border agencies’ ability to have whole-of-supply-chain visibility. This is especially true for business-to-consumer (B2C) shipments which represent great risks to border agencies. Blockchain has the potential to mitigate such risks.

One example of this is in Singapore where they are undertaking an effort focused on the Singapore National Trade Platform (NTP). The platform is an extension of Singapore’s Single Window TradeNet and aims to bring all trade stakeholders onto a single platform to digitize the end-to-end process. The Singapore government is looking to establish a blockchain network with Hong Kong, Netherlands, and Australia with the goal of ensuring all trading partners can share information securely to facilitate trade. Today, document submission and approval processes for sellers, banks, logistics, consumers and government agencies are repeated along the value chain. The platform, powered by blockchain technology, provides a ledger for documents and records that stakeholders can use and reuse without worrying about the integrity of their data and privacy-related issues.

Barriers to Blockchain Adoption

Despite the potential upside to the widespread adoption of blockchain, a few key barriers exist that must be overcome. The first and biggest hurdle is the linking of all physical objects to the information digital stream. Currently, individual items may be tagged digitally with radio-frequency identification (RFID), near field communication (NFC) or a 2-dimensional barcode. However, in order for blockchain to realize its full potential, all products would have to be tagged digitally, requiring an overhaul in today’s supply chain practices. Without an industry and supply-chain-wide commitment to adopt this digitalization, many organizations will not make the investment in this technology.

Similarly, cultural adoption and privacy concerns are additional key barriers that must be addressed. Without strong and reliable safeguards in place, the public may not be amenable to uploading every object’s history into the cloud and having that data stored across various network devices. Furthermore, while the incorruptibility of blockchain is a potential benefit, it may also be seen as a detriment as data cannot be deleted from the chain.

² <https://www2.deloitte.com/us/en/pages/operations/articles/blockchain-supply-chain-innovation.html>

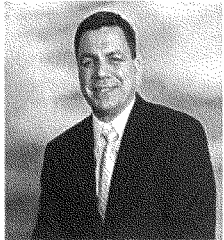
Finally, the international community must come together to ensure there is one unified set of standards for blockchain. This will give companies the confidence they need to know the technology they adopt will be recognized throughout the world. Without these common standards, uncertainty will prevent the large-scale investment that is needed to make blockchain in the supply chain a success.

Conclusion

Thank you once again for inviting me to testify before you on this technology that could change the way the world understands supply chains. I look forward to any questions.

Chris Rubio

Vice President, Global Customs Brokerage Staff



Chris Rubio, Vice President UPS Global Brokerage Staff - is responsible for business ownership, and strategy of the global customs brokerage systems in use by UPS in the 220 countries that we serve.

Chris has been with UPS for 30 years. Chris has 29 years of international industry experience. His career began in 1987 first as a package car driver and shortly thereafter in the UPS Metro NY finance department as an accounting supervisor.

Chris was shortly promoted to International Finance and Accounting Systems Manager position as UPS began to expand its International presence in the late 1980's and early 90's. Chris has held positions of increasing responsibility – integrating acquisitions, launching new services, and initiating/managing multi-country, cross functional technology efforts for UPS International up until serving his current role on the Global Customs Brokerage Staff.

Chris holds a Bachelor's degree in Accounting from Pace University, and an MBA in finance from Rutgers University.

Chairman ABRAHAM. Thank you, Mr. Rubio. And I want to thank all the witnesses again for coming here and certainly bringing your knowledge base to this subcommittee.

If I understand blockchain correctly—and I am in a steep learning curve—but it will revolutionize tracking of goods somewhat like GPS revolutionized navigation. So I think this is world-changing technology that we're dealing with.

I'm going to ask some questions for five minutes. Mr. Chiaviello, I'll ask you first.

In your testimony you detailed the issues your company and others are experiencing with counterfeit goods in the supply chain. What sort of impacts, either quantitative or qualitative, has this had on your business and on your customers?

Mr. CHIAVIELLO. Well, on our business it certainly affects us on the order of millions of dollars a year. I mean, it's hard—it's difficult to put an exact number on it because we don't know what we don't know, but based on what we can determine from what we have investigated, as I say—and it's growing. You know, five years ago, we didn't really see this problem, and—so now it's—it's a million-dollar problem, whereas five years ago, well, it barely existed.

The direct effect is not only does it—it costs us—it costs us money, it affects our competitive situation as these pirates or counterfeiters, they don't bear the cost burden that we do in making sure that our products comply with federal regulations, so they can compete against us with a much lower cost structure. Our products set the—sort of set the price level. They come in just slightly underneath us, but because they don't have our cost structure, it's very, very profitable, which is what's driving this business.

Chairman ABRAHAM. So building off that, Mr. White and Mr. Rubio, how can your companies, with the application of this blockchain technology, help a company that Mr. Chiaviello represents? What can you guys do to combat that counterfeiting of goods?

Mr. WHITE. Well, the platform we're putting together between Maersk and IBM initially is one that helps identify the sources of information. So we use blockchain to help establish who are the—it's a blockchain solution which is permission blockchain, which means that the entities that are involved are known to each other. And if the documents created from origin are sent to anybody else who are party to that transaction, if any of those documents change, it's immediately identified that the document has been changed. And that could work from a change from when it goes to a customs authority or another government agency, when that's been certified and the document is therefore sent down the path.

So the ability to identify any changes in the documentation of what's been shipped or any new entities that are involved in the party is immediately identifiable. So it helps identify the potential risk of fraud I think much easier, much earlier, and for everybody involved in the transaction to see one document is different from what was—the rest of the documents that they had seen up to that point.

Chairman ABRAHAM. Mr. Rubio?

Mr. RUBIO. Yes, and what we can envision is an environment where you can have a provision—permissioned network of traders,

and in this permissioned network of traders, you could have the different actors in the supply chain exchanging information. And as the exchange information, fraud can, you know, immediately be detected via the technology, and then those that fall outside could be, you know, scored negatively and removed from the networks, et cetera. So the technology really lends itself to advancing the internet—intellectual property rights protection, and we see that as a possibility going forward.

Chairman ABRAHAM. And Dr. Maughan, could DHS potentially leverage this blockchain as a tool to combat the importation of counterfeit goods?

Dr. MAUGHAN. Yes, certainly. In fact, if you look at the Customs and Border Protection, they are just one person and one organization involved in the whole transaction, along with companies like Maersk and UPS and others. And so that's the work we've been looking at is in the pilot phase. How could we use the blockchain technology to detect counterfeit goods more easily?

Chairman ABRAHAM. Are you seeing any obstacles that we as a federal government are throwing up in your path to prevent you from using that technology in an efficient and productive way?

Dr. MAUGHAN. To date, no. As I pointed out in my testimony, the one area that does concern us is a shortage or lack of standards, and so we've been focusing on specifications towards that end, and I think when we have a full network of standards that everybody can live by, then I think that will be even more useful for all involved.

Chairman ABRAHAM. Thank you, Dr. Maughan.

I now recognize Ms. Bonamici for 5 minutes.

Ms. BONAMICI. Thank you very much, Mr. Chairman, and thank you to all of our witnesses for your testimony today. There is certainly a wide range of possible applications for blockchain technology, some quite fascinating, for example, safeguarding ownership of creative works or voting technologies. There's a lot of potential there.

These and other possible uses are important, but the health and safety of Americans is of course something that is of paramount importance. So I'd like to focus on one particular area where blockchain may offer benefits, namely drug abuse prevention. I recently had a series of community meetings in northwest Oregon about the toll of the opioid epidemic on our families and our communities, and one issue that came up not infrequently was the influx of dangerous drugs from foreign countries, especially fentanyl from China. So it seems that blockchain could be used to prevent the importation of illicit drugs or the unlawful diversion of legitimate medications.

Parcels that are shipped from foreign countries are a major source of illegal substances, including opioids and, as I mentioned, fentanyl. I understand that Homeland Security, particularly customs, is as concerned about this as I am. And I know there are several legislative proposals to combat this problem. For example, one of the bills I'm cosponsoring is the Synthetics Trafficking and Overdose Prevention Act that would require foreign and postal operators to provide electronic data, enabling Customs and Border Patrol to better target and screen high-risk shipments.

So, Dr. Maughan, might there be uses for blockchain technology in verifying that imported goods are legal and do not pose a threat to public health or safety? And are you aware of efforts or discussions specifically around using blockchain to prevent illegal drug activity, whether it be the interdiction or preventing diversion?

Dr. MAUGHAN. So I am unaware of any activity to date that is looking at this issue, but I certainly believe that it has a very interesting opportunity for us. As I mentioned in my testimony, there are other pilots that we are looking at with CBP to address counterfeit goods. We just haven't had the conversation about the opioids, fentanyl, and other illicit drugs in those types of pilots.

In the end, the goal here is to be able to track goods, not only the—you know, using industry providers as well as government participants, and I certainly believe there's opportunity to look at that in the same example.

Ms. BONAMICI. I think that would be some welcome work. Also, Dr. Maughan, of course food safety, which you mentioned and has been mentioned in the testimony, the FDA and Centers for Disease Control recently warned us all about E. coli contamination in romaine lettuce, for example. Would you be able to comment on how blockchain might improve that ability to ensure food quality and safety? And you mentioned pilots. I know there's a couple of pilots going on and trial projects regarding seafood traceability, working with organizations so that customers, when they're shopping for fish, can know exactly where that came from and trace that. So do—are you aware of that work?

Dr. MAUGHAN. I'm not aware of that work but one of the other witnesses mentioned mangoes. There have been—and avocados. There have been other examples of cases where we've tracked food and goods, and I certainly believe the application areas are unlimited as to how we would use the technology to provide food safety for the Nation.

Ms. BONAMICI. Mr. Rubio, I understand that UPS already requires a kind of electronic registration data from foreign shippers. Could you comment on whether blockchain could play a role in this area?

Mr. RUBIO. Yes. Most definitely, we see the opportunity, again, leveraging the potential of blockchain to provide permissioned access for the exchange of information and then leveraging the information that's—that can be collected to perhaps maybe score customers and then provide access to, you know, secure supply chains.

Ms. BONAMICI. Terrific. And I don't know who wants to weigh in on my next question. As we are talking about this great potential from blockchain, we also understand and talk about in this committee a lot quantum computing and whether the development of blockchain is really keeping up with what's happening with quantum computing. I know NIST, the National Institute of Standards and Technologies, is looking at this, sort of incorporating some quantum cybersecurity measures along the way because everything I've read said that that is the big threat eventually that if we don't keep—as we're developing blockchain if we don't keep up with what's happening with quantum computing. Does anybody know about the work that's going on there as blockchain is developing?

Are we developing these quantum-resistant algorithms? Anybody able to answer that?

Dr. MAUGHAN. I'll give you a shot and try, but—so if you look at the blockchain technology, at its core it's cryptography and the ability to secure the data, and the concern is that our cryptographic systems eventually can be broken using quantum computing, and so the concern is how do I make my cryptographic algorithms at the core of the blockchain technology something that can be quantum-computing-resistant or at least allow the cryptography to be—to last a lot longer. And the concern is if our adversaries are using quantum cryptography to break our cryptographic algorithms, they would actually be able to break the blockchain technology.

Ms. BONAMICI. Certainly something we can discuss further. Thank you. My time is expired. I yield back. Thank you.

Chairman ABRAHAM. Mrs. Comstock.

Mrs. COMSTOCK. Thank you.

Mr. Chiaviello, as a mom and a grandmother now, your testimony about the challenges of knockoff children's products was certainly troubling. So how might the use of blockchain technology help a company resolve this problem? And what other tools might be useful in helping companies and consumers combat counterfeiters particularly in this area?

Mr. CHIAVIELLO. Well, I think the primary goal would be to control access, in other words, as the term has been used, permissioned access. And so when a consumer is—well, let me give you an example. Teethers are regulated by the Food and Drug Administration and require that any factory where a teether is manufactured has to be registered with the Food and Drug Administration, has to pass extensive health and safety evaluations. And then once the factory passes those tests, the factory is given a number. And that number then identifies the source of all the teethers that originate from that factory. And so that number can act as a stamp of approval like USDA approval on hamburger, on beef products and go with the product, using a blockchain technology to assure the consumer that the product they are buying is an authentic product. In other words, it's been—I don't want to say certified but it's—originates from a certified location. So I think there's great opportunity for—in that respect.

Mrs. COMSTOCK. Okay. Thank you. And then I guess for other witnesses, if any of you work—does any of your work involve coordinating with NIST or leading any type of collaboration with other industries regarding standards for blockchain technology?

Mr. WHITE. From Maersk and IBM, we're looking to embrace existing standards, industries, wherever there are standards available so that we can make sure that we adopt and embrace it. In our view, to have a platform that really helps to accelerate the digitization of global trade, we need to be completely open and neutral, and we need to take advantage of having common standards around the world.

So here in the United States we're looking into the BiTA, which is trying to look at some of the standards. Also, we're working with other agencies as they develop across the global economy to understand where those opportunities are. Also, we look to be embracing not only DHS and CBH here—CBP here in the United States but

also other customs and WCO to understand what direction they're going because we think it's really important, this interoperability. We need to make sure that everybody can avail themselves of this platform and exchange information in a transparent way using blockchain that provides that immutable trust.

Mr. RUBIO. Yes, and UPS is also involved in the BiTA Alliance, and we're clearly interested in advancing standards in blockchain.

Mrs. COMSTOCK. Okay. And have your companies recognized any cybersecurity benefits in the development and implementation of blockchain technologies across various applications? That's for any of you.

Mr. WHITE. At this point, we're still in the pilot program of putting together the platform and again waiting for regulatory approval, so it's a little bit early on in that, but I think it was mentioned using cryptography and having a permission blockchain, I think it's a 32-character alphanumeric sequence that has to be attached to the previous documents in there. So, so far, it seems that it's pretty trustworthy in terms of getting that information across there. It's a little bit early to see about the broader applications for cybersecurity, but that's obviously high on our list at Maersk Line, concerning some of the challenges we went through last year, and just make sure that we continue to keep that high on our agenda because it's critical to global supply chains.

Mrs. COMSTOCK. Okay. Anyone else on that? Okay.

Well, I'll yield back, Mr. Chairman. Thanks.

Chairman ABRAHAM. Thank you, Mrs. Comstock.

Dr. Marshall?

Mr. MARSHALL. Thank you, Mr. Chairman. Let me first of all brag on my two grandsons, so congratulations to Mrs. Comstock on a new granddaughter.

Mrs. COMSTOCK. Yes, I have a grandson and a granddaughter—

Mr. MARSHALL. Well, good for you.

Mrs. COMSTOCK. —this past year. Yes, so I—

Mr. MARSHALL. We've both got two each up here. This doesn't count against my time does it?

I want to start with Mr. White. How important is NAFTA to Maersk?

Mr. WHITE. Well, NAFTA is important to all of us. I think, as Maersk, we're obviously supporters of global trade and trying to make sure that, you know, there's opportunities to promote that. In terms of North America, South America, most of our shipments are international by water, so there's some that's moving via that route, but most of that's moving overland borders. So we of course are interested in monitoring that, and we—

Mr. MARSHALL. Okay.

Mr. WHITE. —just support whatever the regulations are and make sure that we can make trade as easy as possible under the regulations that are available.

Mr. MARSHALL. Mr. Rubio, how important is NAFTA to UPS?

Mr. RUBIO. It's very important. Canada's one of our largest trading partners, and of course we move lots of products between United States, Canada, and Mexico. So we're also involved with CBP on some pilot work related to NAFTA.

Mr. MARSHALL. Okay. Yes, China—I mean, Canada actually is our largest trading partner. We export \$280 billion a year to Canada, 230 to Mexico. China is a distant third at about half of those.

Blockchain technology, as we're modernizing the NAFTA agreement, do you feel like we're doing anything to help empower you all? Either one, Mr. White, Mr. Rubio, are we taking blockchain technology—have you had any conversations with Administration if you're allowed to what would allow you to better use blockchain as we modernize this NAFTA agreement?

Mr. RUBIO. We're—yes, as I mentioned, we're working right now with CBP on a pilot related to NAFTA, and it's progressing very well. We think that will have a pilot up and running in the fall time frame, so I think we're getting great support from CBP in this area.

Mr. MARSHALL. Great. And, Mr. White, anything to add there?

Mr. WHITE. Yes, likewise, we're working with Canadian customs and CBP here in the United States to try and look at the documentation that's required for a certain specific commodity segment of that and to see if that can be applicable there and can we actually make that a standard elsewhere. So we're early days, but we're working together on that.

Mr. MARSHALL. So there's a spirit of cooperation in anticipation of this technology from this Administration?

Mr. WHITE. Absolutely.

Mr. MARSHALL. That's great to hear.

Dr. Maughan, let's talk to you for a second. One of my biggest concerns is I go to all my different meetings, different committees, talk to different folks, is when it comes to cybersecurity, let alone blockchain technology is—I'm worried that every department is doing their own thing. Would you—is DHS the leader on these issues? Would—is there some cooperation between your department and the other departments in the Administration, whether it's blockchain technology or cybersecurity?

Dr. MAUGHAN. So I'll answer from two sides. From the science and technology side, there's a lot of coordination and collaboration going on in the interagency and particularly in the blockchain area where we share what's going on across the different agencies. You have NSF and NIST and others also funding research and development in blockchain.

On the operational side, DHS does have the lead on the cybersecurity, as well as with the NIST cybersecurity framework and it's—how it explains cybersecurity. So both operationally and R&D, DHS has a strong position there.

Mr. MARSHALL. Is there a cooperation with the military in what they're doing in these areas with DHS?

Dr. MAUGHAN. That I'm aware of on the research and development side there is because I'm involved in it and we—

Mr. MARSHALL. Okay.

Dr. MAUGHAN. —do things from an interagency perspective. I don't know the details on operationally. I would expect there is, but I don't know the details.

Mr. MARSHALL. Okay. It's been said—I'll stick with you Dr. Maughan—is that China steals \$400-\$600 billion of our technology every year through copyrights or computer software, whatever it is,

explain to me again—you all have touched on it. Go a little bit deeper. How can blockchain technology impact that? And be as specific give me examples if you could.

Dr. MAUGHAN. Sure. So the—if you look at how a blockchain works and the ability for organizations or individuals to put their cryptographic stamp on the data, right, now, if I use it in that way, you as the Chinese or others, wouldn't be able to counterfeit and——

Mr. MARSHALL. So Nike would have their unique encryption, and you knew if you got——

Dr. MAUGHAN. Right.

Mr. MARSHALL. —a pair of Nike shoes from someone that doesn't have that unique encryption, you as a producer would—I mean, not as a producer—you as a wholesaler in America would understand—would see that?

Dr. MAUGHAN. Correct. And if it's not—if it doesn't have the correct data, doesn't have the correct integrity on the data, then someone would be able to tell that you're not the legitimate producer or supplier.

Mr. MARSHALL. Okay. Thank you. I can ask one more question if you're not quite ready.

Tell me—you know, fentanyl is one of my big concerns. Fentanyl is 100, 1,000 times more potent than the typical opioids coming across. You can make this in your garage. It's coming over by the truckloads from China, I'm told. How can blockchain—you know, UPS or DHS—maybe—Mr. Rubio, you're the UPS guy. Any thoughts how blockchain could impact that?

Mr. RUBIO. It's a tricky issue because it's ultimately what gets packed in a carton, and I think that becomes a challenge for us. Blockchain certainly provides the framework for us to begin investigating the contents and then perhaps scoring transactions and then eliminating them from the supply chain. So the framework is there, and it's an area that will require work——

Mr. MARSHALL. Can we trace it backwards, you know, perhaps back to the origin——

Mr. RUBIO. Absolutely.

Mr. MARSHALL. —a little bit better?

Mr. RUBIO. Yes, using the same techniques that Dr. Maughan explained, that's exactly the way we would go.

Mr. MARSHALL. Thank you, Mr. Chairman, and I apologize I went over. I yield back.

Chairman ABRAHAM. That's quite all right, Doctor.

Mr. Hultgren, 5 minutes.

Mr. HULTGREN. Thank you, Chairman. Thank you all. I appreciate you being here. This is a really important, interesting, challenging topic and grateful to learn from you all. And I've also been grateful I've been able to see a number of great ideas coming out of Illinois, my home State, with many investments in the financial sector coming out of Chicago. There are also some efforts at the state level to look at many innovative solutions to state and local government with the Illinois Blockchain Initiative, a consortium of state and county agencies who issued their first report just in February.

I've also been encouraged through the work that I've been able to do on the Tom Lantos Human Rights Commission on the way in which new technologies like blockchain can better secure and validate supply lines in conflict regions, as well as better manage the disbursements of aid through the federal government and other NGOs. The transparency of something like a distributed ledger can also give new tools for individuals to finally assert basic property rights when governments deny the rule of law or access to the legal system in other countries.

If I can address first, Mr. White, Mr. Rubio, and Dr. Maughan. Previous witnesses before the Committee have detailed how thoughtfully inserting blockchain, inappropriate projects already funded would ensure we stay at the forefront of this transformative technology. Have you taken this approach to analyze blockchain's potential for appropriate projects? And in your opinion, what are some examples of where it would be appropriate or not be appropriate to implement blockchain technology? And what's the distinction of where it would work likely and where it would likely not work?

Mr. WHITE. Well, from a Maersk Line perspective, one of the opportunities we see are global supply chains. So global supply chains are some of the most complex multiparty networks in the economic landscape today. So, by definition, you have a number of companies that are involved, transmitting sensitive information for the cargo across different channels. I think blockchain is especially suitable for that because you can enable, through this permissioned blockchain, the entities that should have a right to see and have access to that information, to have access to that information, to make sure that they can see it, and trust that the information has not been tampered with or modified in any way, shape, or form. And then you can tie the visibility of the sort of end-to-end, in-transit information and have that simultaneously with the documents or the data on that to actually enable smoother supply chains but also in a trusted immutable way. So we think for that blockchain is very much fit for purpose, and I think it can be a game changer because it provides that immutable trust through the distributed ledger, through smart contracts, and through a permissioned blockchain, so we think there's a great opportunity.

Mr. HULTGREN. Great. Mr. Rubio or Dr. Maughan?

Mr. RUBIO. Yes. From our side, really it's about reducing friction in the supply chain and streamlining the exchange of information. So what blockchain provides is the opportunity to digitize transactions and then share that information through the network. And as we can collect information near real-time, that will just speed up supply chains and provide, you know, fast-moving product.

Mr. HULTGREN. Okay. Dr. Maughan?

Dr. MAUGHAN. As I mentioned in my testimony, there are other additional ones from a DHS perspective in addition to the supply chain, but certainly the ones we've been working on is the data and sharing of imagery on the border with CBP in order to be able to share that and ensure the authenticity and integrity of that data. And I think that has tremendous value as we think about IOT devices that are doing—that are collecting data and sharing that data. We'll be able to protect that. There are others that have to

do with passenger processing and other aspects that I think our potential uses as well.

Mr. HULTGREN. Yes. Any that jump to mind that you feel like this just wouldn't work? It's just not the right place for this? I guess if that comes up, let us know because we definitely respect your thoughts and opinions.

Let me move on in my last minute here again to Mr. White, Mr. Rubio, and Dr. Maughan. Do you collaborate or coordinate with any domestic or international standards bodies on blockchain?

Mr. WHITE. Yes, so from a Maersk Line and IBM association, we're working together and looking to work with BiTA here in the United States and also looking to work with other entities around the world. We think it's very important to have sort of a common definition of standards where standards exist, and where standards don't exist or need to be improved, we want to work collaboratively with others to make sure that we get the right standards so that we can all—make sure that we can talk more easily through a digitized environment going forward.

Mr. RUBIO. UPS is also a member of the BiTA, and we're very interested in driving standards to improve this technology.

Dr. MAUGHAN. And we are actively involved with both the World Wide Web Consortium, the W3C, and OASIS, the Organization for Structured Information Systems for some of our standards work as well.

Mr. HULTGREN. Great. My time is expired. Thank you again for your work. Thank you, Chairman, for holding this hearing.

Chairman ABRAHAM. Thank you. Mr. Beyer?

Mr. BEYER. Thank you, Mr. Chairman.

Dr. Maughan, you—in your briefing you said, and I quote, "Most organizations don't need a blockchain." Can you tell us why most organizations don't need a blockchain?

Dr. MAUGHAN. So we've worked through kind of a process to ask some questions of people about what they're trying to do, and they oftentimes don't need a blockchain. They can solve their problems with a database or other accounting instruments. And it takes a little bit of a discussion to get to a point. A lot of times people are thinking just in a single organization they'll use a blockchain. Well, they don't really need one. The blockchain, its attributes include multiple parties, trust relationships, and different types of sharing of information and storage of information. And you really need to actually walk through a certain set of questions to decide whether you really need a blockchain. And in a lot of cases, people don't need a blockchain.

Mr. BEYER. You know, there have been lots of anxiety the last couple of elections—and not just 2016—2004, 2008 about the security of voting machines, and there's a move to online voting but only if it's secure. Is voting someplace where blockchain might be relevant or is this like again a place where there are other simpler technologies?

Dr. MAUGHAN. I think we're early days. I don't know that we've done the real diligence that we need to look at that, but I actually believe that voting is probably not a place where we would use blockchain technology.

Mr. BEYER. Would every voter have to have their own blockchain key and—

Dr. MAUGHAN. Right, well, the question is, is who am I sharing my vote with? I mean, the only person that I really want to share my vote with is my local voting establishment, and so I think the complexity there is even worse than what we have today in just paper in normal elections.

Mr. BEYER. Thank you. Mr. Chiaviello, you are—I very much empathize with the problems of your company. I'm an automobile dealer, so counterfeit parts have plagued me for more than 4 decades. But are any of the companies that you represent now pursuing blockchain technology? And do—on the other hand, if you complain about reselling the counterfeits through a big company, an Amazon, do they have to be a participant in the blockchain with you to make this work?

Mr. CHIAVIELLO. I—we are not pursuing blockchain at this point directly, but it would appear that the retailer, the Amazons of the world, would have to be participants in blockchain technology. And we would have to be participants as well. As we see it, where this is going is that the blockchain, the key to a blockchain would be like a digital hologram or an equivalent to a trademark or a watermark that you might find on paper identifying the product itself as an authentic, legitimate product. That would have to be established by someone like us, the designer/manufacturer, but then it would have to pass through the entire supply chain, and ultimately, we would need a method for the consumer to be able to verify that that product is a legitimate, authentic product.

Mr. BEYER. Interesting. Mr. White, you have your—you had global perspective with Maersk obviously, and I strongly believe, just based on this committee's interest, that America should take the lead on blockchain innovation research. But we have—we see what a lot of the other nations are doing. China recently launched what they call the Trusted Blockchain Open Lab. Dubai says it will be the world's first blockchain-powered government. Singapore is exploring it. Russia's state-run bank Sberbank announced it's going to team up to do blockchain for document transfer. The European Union launched its E.U. Blockchain Observatory and Forum. Where is the United States compared to the rest of the world in terms of our blockchain leadership in research?

Mr. WHITE. Well, I think the United States is leading in lots of ways on blockchain. Maersk and IBM are coming together for our collaborative effort that we are seeking regulatory approval in different authorities around the world to launch this global digitization platform I think is evidence of the largest marine transport container shipping company in the world and the technology giant of IBM that is a leader in blockchain coming together to have some innovative uses of blockchain.

And it's not—I would say blockchain is not a solution looking for a problem. It is specifically fit for purpose for a global supply chain, so when we talk about this large, distributed network, multiple parties transmitting sensitive information across not only organizational but also geographical boundaries, having some way to do that in a secure manner I think helps facilitate trade. I think it helps to certainly identify fraud much earlier in the process, which

is a significant disincentive to it. And I think we can create safer, better, more efficient supply chains by deploying this technology. And I think the United States is right in the forefront of that.

Mr. BEYER. Thank you. Mr. Chairman, I yield back.

Chairman ABRAHAM. Thank you. Mr. Loudermilk?

Mr. LOUDERMILK. Thank you, Mr. Chairman. And first of all, I want to thank the Chairman for holding this hearing. I've kind of felt a little bit like a voice in the wilderness on blockchain—excuse me—after spending 20 years in the—20-plus years in the IT industry. And I've often said for the last couple of years if we can get over the stigma of cryptocurrency and look at the technology beneath it, it could be a solution to a lot of our cybersecurity and data protection issues.

And so I appreciate the Chairman having this hearing. I was very excited when I saw it because I think we're beginning to make some progress from this side of the dais in looking at this incredible technology.

Mr. Chiaviello, you talked about counterfeit and knockoff products as a problem, the sale and distribution of those. Can you elaborate a little bit how the sell and distribution of these counterfeit goods makes it difficult and costly to police and enforce IP rights, intellectual property?

Mr. CHIAVIELLO. Yes. The big problem that we're facing now is that the—the pirates, the knockoff companies are now located overseas, and we have no way of identifying them. They establish an online store with typically a fake name and no identifying or contact information. The—if they have a domain name, it's hidden behind a proxy server, privacy proxy, and so we have—we or the consumer have no way of identifying where that entity is located.

Products that are shipped into this country, often they use fake addresses. Return addresses on the packaging are fake, and so we and the U.S. consumer is essentially left without a remedy. There's—as you know, to bring an action in a federal court or even a state court, you need personal jurisdiction over the seller.

Mr. LOUDERMILK. Right.

Mr. CHIAVIELLO. And if we don't even know who the seller is, much less where they're located, we cannot get personal jurisdiction, and any default judgment would be essentially valueless trying to enforce it.

Mr. LOUDERMILK. What would be the long-term consequences of failing to address the issue both to business and to the consumers?

Mr. CHIAVIELLO. Well, it puts domestic companies at a financial disadvantage. We're competing with people who don't incur the cost for the R&D, don't incur the cost for the regulatory compliance. And at the least it limits our growth. We're not as—we cannot be as big company as we should be based on this type of foreign unfair competition. And to the extent it continues, it threatens domestic industries.

Mr. LOUDERMILK. Okay. Thank you. Let me steer a little closer back to Georgia with our good corporate partner from Atlanta. Mr. Rubio, you've stated or actually wrote that blockchain could make large multinational companies such as UPS more efficient and could, and I quote, "leave them better equipped to handle the continued growth of e-commerce." Can you elaborate a little bit more

on the e-commerce aspect of that and how it can help these companies be more efficient, as well as more secure?

Mr. RUBIO. Sure. The promise of blockchain is that it allows for the digitization of transactions within the supply chain. And in the e-commerce space, oftentimes documentation is required to clear customs around the world. And so what blockchain can do is it can provide the vehicle for us to digitize transactions, collect that information, and make it simpler for the consumers and then eliminate this friction in the supply chain. So by posting information in real time to the supply chain, data can be shared among the different players, and that would streamline the flow of goods.

Mr. LOUDERMILK. What's the benefit to the consumer?

Mr. RUBIO. The benefit to the consumer is that they can receive their product quicker without any interruption.

Mr. LOUDERMILK. All right. Thank you. Mr. Chairman, I yield back.

Chairman ABRAHAM. Thank you. Fascinating subject, so we're going to have another round of questions here.

I'm sure volumes have been written on the efficiency of both Maersk and UPS as far as moving goods, phenomenal companies. But, Mr. White, in your testimony you said that blockchain technology could increase global trade by up to 15 percent. That's a phenomenal figure, and certainly we want to move that forward. One barrier to the widespread adoption of blockchain technology is the linking of the physical object to the digitization. Can you guys—Mr. White and Mr. Rubio—can you all elaborate as to how we can actually make that happen, how we can make those physical dots connect?

Mr. WHITE. I think it's well-cited. Actually, during our evaluation of supply chains, we looked at some of the most sort of complex supply chains, as I mentioned. You have a challenge of both the physical end-to-end transport of the goods, which is one thing, and the visibility of the events that—the real-time access of that information as to where that container in our case is physically located at any one point in time and then the disconnect that we see from a paper-based documentation flow, so linking the two of them together with digitization so you have the opportunity to have more real-time visibility as to where a shipment is.

So with our platform we have a shipment—shipping information pipeline, so we can actually see more events of what's happening with that container, everything from when it's empty for loading to when it's stuffed to when it's back to the terminal facility to when it's loaded on board a vessel and onto any train shipment through customs clearances on both ends, endgame delivery, but also having the capability with this platform to have digitize documents. As Mr. Rubio has said, it enables us to have them in a structured way in a format that the government agencies require so that they can actually process them. So you have the capability of having them both together.

In our supply chain evaluation, the one shipment of avocados I mentioned was I know is a 34-day end-to-end transit from when it was actually farmed at the farm and then put to the truck to be loaded into a container until it would end up being delivered. In that 34 days, 14 days, two weeks of it, it was sitting there waiting

for documentation for processing. So you've got an opportunity to actually improve supply chain cycle times and the efficiency, as I mentioned, over 200 individual exchanges of document and information. With the certifications that were required, they actually are stamped by one authority and moved by courier by motorbike to another authority for another stamp and then to the port so you're physically moving documents instead of transmitting electronically.

Chairman ABRAHAM. Mr. Rubio, do you want to weigh in on that?

Mr. RUBIO. Sure, yes. The big challenge of course is making the physical world connect with the information world, and that really is a key challenge that will need to be overcome in order to achieve the ends that you're asking about.

But there are technologies that can speak to the data like RFID, as I mentioned, and potentially even x-ray technology. So x-ray technology, you know, the possibilities exist for interpretation of x-rays to understand what's actually in a carton and then leveraging that information with what's physically been communicated by the different players in the supply chain can then further support the validity of what has been claimed on the transaction. So those are kinds of techniques that can be used to link up the two. It's a very tricky issue, but that would be how it could possibly unfold.

Chairman ABRAHAM. All right, thank you. Dr. Maughan, we have consistently heard that in order to effectively foster the adoption of blockchain solutions to supply-chain problems, there must be a common set of standards, and we've addressed that somewhat here today that are globally recognized. How can such standards be promulgated and adopted?

Dr. MAUGHAN. First is the development of those standards, which we're working on with some of our partners, but then I think it is—it's an education game. As you can tell, we're fairly early on in the blockchain world, and it becomes up to companies like Maersk and UPS as they use it to educate others. And I think we are in a leading position within the world that we the United States can take a leadership role and continue to push blockchain and educate people on the use of it.

Chairman ABRAHAM. So you agree that the United States should lead that charge?

Mr. RUBIO. I certainly believe we should take a leadership role. I don't know if we're going to be out in front because you can't do a blockchain by yourself, right?

Chairman ABRAHAM. Right.

Mr. RUBIO. I mean, what we want to do is have this conversation both government to government and have a conversation with our government partners so that they are also on board because it is a global community.

Chairman ABRAHAM. Okay. Thank you. Mr. Beyer?

Mr. BEYER. Thank you, Mr. Chairman.

Mr. Rubio, you talked about how UPS is committed to blockchain, and you also talked about some of the obstacles. One of the things I read is that Visa right now can process 56,000 transactions per second, but the Bitcoin blockchain is only about

five transactions per second. Do you see this transaction processing power an obstacle to making UPS effectively use blockchain?

Mr. RUBIO. Well, I'm unfortunately not in a position to qualify any statements on Bitcoin, but certainly, the blockchain itself, we certainly see the capability to share information, streamline information, and process it in real time and absolutely by exchanging information rapidly, that will streamline the supply chain and allow trade to happen efficiently.

Mr. BEYER. If you adopt blockchain, will UPS drivers be allowed to turn left?

Mr. RUBIO. Hardly.

Mr. BEYER. Okay. Dr. Maughan, one of the things that—you know, when we had our last blockchain technology, we got all excited for two hours and somebody pointed out that when quantum computing comes, that it goes so fast that they actually break the block chain keys. How soon do you see this coming? Do—does it make sense for us to make all this huge investment of blockchain if quantum computing is going to make it irrelevant once it arrives?

Dr. MAUGHAN. You know, that's a very good question, and I think we don't know yet where—when quantum is going to be here, right? I mean, it depends on who you talk to. Quantum is 10 to 15 to 20 years out, and there's still I think a lot of research and development to be done even to get us there. And I think the issue is blockchain today can use cryptographic algorithms of today and still provide us the security and the privacy we need? I think we're going to have to figure out how this competition, if you will, between blockchain and quantum, how that plays out over the next decade or two.

Mr. BEYER. Blockchain at least is a lot more intuitive—

Dr. MAUGHAN. It is and—

Mr. BEYER. —than quantum entanglement and things like that so—

Dr. MAUGHAN. That's right, a bit easier to understand.

Mr. BEYER. So you have this beautiful education, a Ph.D. in computer science. The President still doesn't have a National Science Director, head of the Office of Science and Technology Policy at the White House. Are you—should you apply? It would be the first computer scientist ever to be the White House Chief Scientist.

Dr. MAUGHAN. I don't think I can comment on that.

Mr. BEYER. I'm talking to my friend here, the Chairman. I yield back, sir.

Chairman ABRAHAM. Thank you, Mr. Beyer.

Mr. Hultgren?

Mr. HULTGREN. Thank you again, Chairman.

Moving on to a couple other questions I had, so, first, I'm going to address this to Dr. Maughan. Other experts in the field have noted the potential opportunity for nurturing future blockchain projects within SBIR, the Small Business Innovation Research program. Do you see any other areas within the federal government that could help facilitate the establishment of blockchain projects or pilots, certainly within DHS but other spots as well?

Dr. MAUGHAN. I think the applications are almost limitless, and I think the question is really up to the departments or agencies as

to how they try to address that. We have—from a science and technology perspective, we have taken a fairly good leadership position so far within the government. We are talking about other applications where blockchains might be usable, and we have also used our Silicon Valley Innovation Program to fund startup companies to look at some of these techniques and technologies. In fact, the pilot we're doing with the Border Patrol on data imagery is with a startup company out of Texas.

Mr. HULTGREN. Great. Thank you. Mr. White and Mr. Rubio, specifically with respect to collaboration and standardization, what are some of the lessons your companies have learned that will help you utilize blockchain technology at scale?

Mr. WHITE. So in terms of lessons, I think this item of standardization is critically important. We need to understand what standards are out there. For instance, you know, if we look at just end-to-end supply chains, UNC codes or the way that we define inland points varies depending on what geography you're in, and then also are they specific enough to really nail down, you know, what the geography is that you're—if you're talking about multiple facilities within a common ZIP Code, for instance. So the ability to sort of embrace and tackle some of those challenges I think, as an industry, we have to do it. It's something of course Maersk and UPS could do individually, but then if we're both calling it something different, it makes it a challenge. So I think coming together, working through these advisory boards and these standards committees, I think it's really important to prioritize what are the most important standards to get alignment on and how can we move that forward.

And in addition to joining these established organizations between Maersk and IBM with our new platform we're looking to establish an industry advisory board, you know, making sure that we have participants from ports, terminals, other carriers, inland carriers, customs entities if we can to make sure that we look at it from a collaborative multi-perspective position.

Mr. HULTGREN. Thanks.

Mr. RUBIO. And the lessons that I'm learning personally in this space being involved in some of these working committees, but as you sit through and you look at defining standards for how we're going to communicate and collaborate via blockchain, there are painstaking issues over data that you will exchange. And so it's fascinating to listen to the different players and their perspectives of what information would be useful to exchange and what information would not. So it is—in driving the standards, it's not a trivial task but it's an important task. And in the end, you end up with a very sound product. And my first-hand experience is that's how we did it with CBP, and you guys should be proud of the work that they have done so far.

Mr. HULTGREN. Absolutely. Thank you. One last question, again, Mr. White, Mr. Rubio, and Dr. Maughan. Given its jurisdiction over NIST, what can this committee do to ensure that the United States is cultivating a supportive environment for blockchain technology projects? Dr. Maughan, I'll start with you.

Dr. MAUGHAN. Well, I think certainly in our role within DHS, we work a lot with NIST and the roles there. They've published docu-

ments identifying blockchain overview and how that all works, and I think just to continue participation in the standards community is an important part for NIST participation, and we've certainly been working with them on that.

Mr. HULTGREN. Great. Thanks.

Mr. WHITE. The interaction we've had with DHS and CBP has been very positive. We've been working with the E.U. CORE project for the last 18 months to try and understand how they're approaching digitization, and CBP and DHS have been supportive of that. And then also as we're developing our platform trying to learn from those lessons, that continued support and looking to how we can work with other partner government agencies, I think they have been very constructive in that process.

Mr. HULTGREN. Great. Thank you all so much. I'll yield back.

Chairman ABRAHAM. Thank you. Mr. McNerney?

Mr. MCNERNEY. Well, I thank the Chairman and I thank the panelists.

Mr. Rubio, can you walk us through why blockchain technology is useful for identifying—for identity verification and why this is important for chain logistics?

Mr. RUBIO. So it's—it would be important for identity verification in that it would help secure supply chains. And so understanding who the actors are in the supply chain that are exchanging product or information would be critically important so that we can maintain security and it can also be leveraged for potential intellectual property rights types of issues.

Mr. MCNERNEY. Good. Thank you. Mr. Maughan, is the U.S. Government currently using blockchain technology to mitigate cybersecurity threats?

Dr. MAUGHAN. I'm not aware of actual deployed blockchain technology. As I mentioned in my testimony, we have a number of pilot deployments where we're testing out some of the technology to see how it will be used and the scale at which we can use it.

Mr. MCNERNEY. Are there any potential risks associated with using blockchains to reduce cybersecurity threats?

Dr. MAUGHAN. I don't know that there are that many risks. I mean, I think we're—you know, when you start talking about cybersecurity, it is about the data and can I ensure integrity and authenticity? As long as the technology is implemented correctly, then I think the risks are—they're mitigated by the technology itself. A lot of times in cybersecurity the problem is implementation and people implementing it incorrectly.

Mr. MCNERNEY. I understand. I'm not sure which panelist to ask, but could someone discuss the energy implications of expanding applications of blockchain technology and how can it be mitigated? Who would be the right person to address that? What are the energy implications of blockchain—widespread application of blockchains?

Dr. MAUGHAN. I believe your question is probably related to—if you look at from an energy standpoint, are you talking about computing power?

Mr. MCNERNEY. Right.

Dr. MAUGHAN. Yes. So if you look at the way cryptocurrencies are used—and there's an awful lot of computing power in the back-

ground of cryptocurrencies to actually make them work. And so the—I think the question and the discussion is about if I start to do large-scale blockchains, I now have computing infrastructure that I also have to operate. And the question is does that make it a difficulty for a small business or someone else to ensure that they have the adequate power to do their blockchain technology? Because you do have to check. And there's checks all along the way in the data to ensure that it hasn't changed and that—and it is authentic, and so there is a computing infrastructure that goes along with this. It doesn't just happen.

Mr. MCNERNEY. So, I mean, what can be done to mitigate the energy usage implications of widespread application of blockchains?

Dr. MAUGHAN. I actually believe you're going to see companies like Maersk and UPS probably have their own large infrastructure from a computing standpoint. I think you have a potential for service companies to provide, which is what happens in the cryptocurrency world. There are what are called Bitcoin miners, and they run the infrastructure that does a lot of the calculation.

Mr. MCNERNEY. Right.

Dr. MAUGHAN. You could very easily see something similar in the blockchain world where someone else is doing—offering a technical capability to provide you a service and be the computing infrastructure if you are a small business.

Mr. MCNERNEY. Mr. White, I have in my district the Port of Stockton. It's the largest inland port on the West Coast. It's the third-largest port in the State of California. What steps is your company taking to increase adoption of blockchain technology?

Mr. WHITE. Well, we're working with ecosystem participants from ports and terminals to major rail operators, so we're already in discussion with four out of the seven class I railroads in the United States and also with trucking communities because we think by everybody participating in this new global platform, we have the capability of making it more visible in terms of the seamless and more efficient movement of cargo and, by using blockchain, make sure that those who are permissioned—it is a permissioned blockchain, so those who are party to the shipment can see the information; others cannot. And those that can see it can get better real-time information, so in terms of moving cargo efficiently through ocean or inland terminals, getting better visibility as to when cargo is available, will be available, and enabling more efficient use of the landside equipment that moves cargo between the ports and the shippers or the consignees and D.C.'s and warehouses.

Mr. MCNERNEY. It sounds like a lot of advantage.

Mr. WHITE. We think it's a great utility for everybody. I think this industry has not really changed since the 1950s since containerization has come around, and I think this technology affords us an opportunity to look at things differently. And what we're seeing is a lot of engagement from everybody involved in the supply chain because I think the industry is ready for change.

Mr. MCNERNEY. Thank you. I yield back.

Chairman ABRAHAM. Thank you, Mr. McNerney.

Well, once again, I thank the witnesses and the members had some great questions. Robert, tell everybody in Monroe, Louisiana, give them my regards. I'll be home shortly.

Mr. Rubio, is that your family behind you?

Mr. RUBIO. It is, yes.

Chairman ABRAHAM. I tell you, I've been watching those two young people. They are our future, and they have been listening intently, so they are our future blockchainers and quantum computer tacticians, so I appreciate their presence very much here.

Mr. RUBIO. Thank you, Mr. Abraham.

Chairman ABRAHAM. The record will remain open for two weeks for additional comments and written questions from members. This hearing is adjourned.

[Whereupon, at 11:32 a.m., the Subcommittees were adjourned.]

Appendix I

ANSWERS TO POST-HEARING QUESTIONS

ANSWERS TO POST-HEARING QUESTIONS

*Responses by Dr. Douglas Maughan***HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY***“Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods”*

Dr. Douglas Maughan, Cyber Security Division Director, Science and Technology Directorate,
Department of Homeland Security

Questions Submitted by Ranking Member Daniel Lipinski,
Subcommittee on Research & Technology,
House Committee on Science, Space, and Technology

1. Although blockchain technology is becoming more widely accepted as a security-enhancing technology for commercial transactions such as bitcoin and health records, its potential applications in the national security industrial base and supply chain are still relatively unknown and unproven. Federal agencies may be reluctant to adopt blockchain or to connect their systems to private sector shipping and logistics chains without prior experimentation and evaluation. Last year, the Department of Homeland Security Science & Technology Directorate awarded several Phase 2 Small Business Innovation Research awards of \$750,000 each to small businesses in hopes of addressing issues related to blockchain use, including cases that involve the movement of people and goods. How else might the government leverage its investments in technology development and testbeds, such as the DHS's university-based Centers of Excellence and the DOD's Digital Manufacturing and Design Innovation Institute (DMDII), which recently received additional funding to jump-start a "Cyber Hub for Manufacturing," to test and build trust in blockchain technologies prior to implementing them in federal and national security supply chains?

Answer:

The Science and Technology Directorate's (S&T) SBIR Awards referenced above include the following projects funded by our Cybersecurity Division:

- Decentralized Identifiers (DIDs) – On the standardization track through the World Wide Web Consortium (W3C)
- Verifiable Credential Data Model – On the standardization track through the World Wide Web Consortium (W3C)
- Decentralized Key Management System – Least Mature; Potential path to standardization via the Organization for the Advancement of Structured Information Standards (OASIS). Design and Architecture is now available for public review

In addition to these, S&T manages the Critical Infrastructure Resilience Institute (CIRI) Center of Excellence, led by the University of Illinois (UI). S&T is working with CIRI and the private sector to test prototype software solutions to support risk reduction in cyber-physical systems. Through this partnership, S&T, CIRI, and UI Labs' Digital Manufacturing and Design Innovation Institute (DMDII) are hosting a joint workshop in

Q1 of FY19 or Q4 of CY18 to assess the potential utility for several of the S&T-funded CIRI projects to support manufacturers' interpretation implementation, and benchmark progress against the National Institute of Standards and Technology's Cyber Security Framework.

As government agencies build and test blockchain technologies in their environments, they should consider incorporating these specifications into their implementations and ensure that the lessons learned be conveyed to the standards organizations to ensure that the final standards support and reflect on the ground implementations. In addition, agency officials should consider engaging with blockchain technology providers to convey the need to support specifications in their products to ensure they are not locked into a particular vendor's implementation. Government agencies should actively engage with the standards organizations to ensure that their use cases and needs are supported by these specifications as they evolve to become standards.

In March of this year, S&T briefed DMDII leadership on S&T's cybersecurity portfolio. Additional discussions are ongoing and joint efforts will be considered where possible.

2. What potential do you see for blockchain technology to improve government supply chains, keeping in mind that the government delivers many "products" such as services, data, and tangible things, that have long supply chains? How can private sector advances in blockchain for supply chain management be leveraged by the government, either to improve interactions with the private sector or to re-engineer government processes?

Answer: Blockchain technology holds the potential for enhanced transparency and auditing of public service operations, greater supply chain visibility to combat the distribution of counterfeit products, and automation of paper-based processes to improve delivery of services to organizations and citizens. When it comes to supply chains, it is useful to differentiate between the tracking of digital and physical assets.

- The tracking of digital assets is often connected to an improved auditing function related to the automation of paper-based processes. There are many places where this is useful and relevant providing that the use case involves multiple parties who do not wish to have a shared infrastructure owned and operated by a single entity. From Dr. Maughan's original testimony, we are currently executing the highest priority proof of concept which is to track free trade qualifications of imported goods by providing greater supply chain visibility, which would answer the following question, "Can distributed ledger technology be used to verify that an item qualifies for a free trade import tax exemption by demonstrating that the necessary percentage of an item's components were produced/assembled in a Free Trade Agreement country?" For this first Customs use-case, we are currently in the proof-of-concept phase, and are testing certificates associated with two particular Free Trade Agreements: the North American Free Trade Agreement (NAFTA) and the Central America Free Trade Agreement (CAFTA). Recently, S&T and CBP held a 2-day exchange meeting to discuss the technical requirements with the various trade and policy groups. The project has transitioned from the operational design phase to the technical requirements development and testing phase.

There will be careful analysis of the success metrics at the end of this phase that will result in a GO/No-Go decision for the next phase.

- The tracking of physical assets tends to be more complicated since it has technical and process oriented dependencies that are outside the scope of blockchain technologies. For example, in order to ensure that a physical asset can be tracked on the blockchain, there is a requirement to uniquely identify the physical asset and to put into place a secure process by which the identifier of the physical asset is tracked digitally on the blockchain. These aspects are not directly blockchain related, and if done in a manner that is susceptible to spoofing (i.e. someone swapping the physical asset but continuing to use the original identifier), could result in an immutable chain of fake data about a physical asset being tracked. Given these dependencies, it will be important for the government to work together with the private sector to integrate technologies that support Non-Person Entity identity with blockchain technologies and to develop and enhance physical-to-digital secure linking processes.

S&T has a number of existing mechanisms available to leverage private sector advancements in technology. For proofs-of-concept and prototyping, Small Business Innovation Research vehicles and the Silicon Valley Innovation Program can be used to explore innovation. Long Range and Targeted Broad Agency Announcements may also be used to support basic and applied research and development activities, unique prototype development, and improving mature technologies for specific homeland security requirements.

Responses by Mr. Robert Chiaviello

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods"

Mr. Robert Chiaviello, IPR Counsel, NUBY Law

Questions Submitted by Ranking Member Daniel Lipinski,
Subcommittee on Research & Technology,
House Committee on Science, Space, and Technology

1. What potential do you see for blockchain technology to improve government supply chains, keeping in mind that the government delivers many "products" such as services, data, and tangible things, that have long supply chains? How can private sector advances in blockchain for supply chain management be leveraged by the government, either to improve interactions with the private sector or to re-engineer government processes?

Answer: While blockchain technology and government supply chains are outside my expertise and the expertise of the client I represent, it does appear that blockchain technology offers a method for insuring the legitimacy and authenticity of goods in general and that should have a positive impact on the security of the supply chain. It would be expected that these benefits would apply to both the private and public sectors. So, development of blockchain technology suitable for the consumer products industry would likely improve government supply chains. The problem that blockchain can solve is the authentication of legitimate products and the validation of authorized and responsible sellers. Authentication and validation are necessary regardless of where the product is made or by whom it is manufactured.

There are two key challenges for blockchain technology before it would receive widespread adoption for low cost consumer products.¹ First, the transaction cost would have to be dramatically reduced and second, the processing capability and speed would have to be increased by many orders of magnitude. With regard to transaction costs, it already appears that there is a pathway currently under development that uses blockchain to authenticate large value shipments such as those generally transported by container. While this is a definite positive step for the consumer products industry, it does not necessarily address the growing problem of direct shipment of counterfeit or illicit products to US consumers from pirates located outside the United States. We leave it to those primarily involved in supply chain logistics such as Maersk to address this issue.

What is needed to protect US consumers and legitimate sellers is a simple, reliable and cost-effective way of authenticating online a single branded product as originating from the brand owner and a responsible seller.² Today, while block chain is certainly reliable, it is neither simple nor cost effective for the authentication of individual consumer products, however the future holds great promise that the technology could meet these challenges. With respect to simplicity, blockchain would appear to be potentially useful for authenticating products from online sellers. An online seller seeking to sell a branded product could be authenticated by the brand owner using a blockchain system that connects the seller to the brand owner. A consumer seeking to purchase the branded product from the authorized seller would be provided the brand owner's certificate that would have to match the certificate issued by the brand owner to the seller and could be verified by the brand owner.

¹ By low cost, we mean products selling for under \$5.00 at retail.

² We have not seen a blockchain technology that would be useful in connection with individual packaging. It appears that for blockchain to work it would require a serialized identification number providing a unique id for each package. Today the cost of such a requirement is cost prohibitive for low cost consumer products.

Assuming blockchain technology can solve the challenges associated with processing capability and speed, it is expected that seller certification and the authentication of the seller's products could be accomplished online with little to no marginal cost. In such a situation, blockchain is a viable solution.

It should also be understood that seller verification does not provide a complete solution as it does not necessarily protect against false or fraudulent data being used at the outset of a transaction. This issue needs to be addressed by international and domestic carriers and postal services. One way this problem can be addressed is for the carriers and postal services to verify the identity of their shippers. It is believed that blockchain would be useful in providing a means for registering shippers and creating a viable audit trail so that a shipper can be held accountable for the products shipped to US consumers from outside the United States. Today, counterfeiters and other illicit sellers use anonymity as a way of preventing accountability. A shipper can generally use a false address as a viable way of creating anonymity. Requiring all shippers who wish to ship products to the United States to register with an appropriate US agency could potentially be achieved using blockchain technology. Such a system would likely address privacy concerns but balance the consumer's need for verifying responsibility. Such a system would certainly allow US consumers to verify the legitimacy of the seller as a reliable and responsible seller.

We understand that blockchain technology is in need of substantial development before it would be suitable for the consumer products industry, but the future looks promising. The Committee's work in this area makes us hopeful that blockchain will be a solution to the rising problem of direct shipment of counterfeit and illicit products to US consumers. We are happy to assist the Committee in its investigation and work aimed at solving this important problem.

Responses by Mr. Michael White

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

“Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods”

Mr. Michael White, Head of Global Trade Digitization, A.P. Moller – Maersk Transport & Logistics

Questions Submitted by Ranking Member Daniel Lipinski,
Subcommittee on Research & Technology,
House Committee on Science, Space, and Technology

1. What potential do you see for blockchain technology to improve government supply chains, keeping in mind that the government delivers many “products” such as services, data, and tangible things, that have long supply chains?

Answer: When used as part of a permissioned blockchain, the distributed ledger created by blockchain technology can bring structure to lengthy, disorganized supply chains. Collecting disparate, siloed data and communication streams in the central, secure, immutable permissioned location of the GTD platform will provide end-to-end visibility on government supply chains. This increased visibility will yield more comprehensive audits leading to earlier and more successful fraud detection as well as incremental efficiency improvements and cost savings at each step in the chain. In addition, both governmental and private entities will be able to leverage the centralized information on the platform to create applications to drive previously impracticable solutions in supply chain technology. One example of this is the possibility for “smart contracts” in which separate supply chain participants are able to fulfill a series of individual conditions in order to “activate” a contract or process such as customs clearance. For example: One government entity with whom we are working experiences delayed shipments at some foreign ports due to incomplete information in shipping documents, creating major disruptions in the supply chain. The reason for this appears to be that, because goods shipped by the government entity are not subject to duties on either end of the supply chain, originators of the necessary shipping documents often neglect to fill in the information (such as a commodity description) required to release cargo at its final destination. With GTD’s Paperless trade solution, the documents could be uploaded directly to the platform by their originator, allowing the government entity to review the blockchain to quickly identify who is responsible for incomplete documentation. Taking this a step further, the entity might eventually use the GTD platform to implement a “smart contract” pursuant to which shipping documents could not be uploaded until they contain all information necessary to release the cargo at its destination. In addition, blockchain technology can be used to encrypt and preserve data products in the same manner that it preserves specific data and documents related to tangible property. In the near future we anticipate that the platform will be able to handle strings of data which, while not necessarily related to specific containers or tangible

goods in transit, will nonetheless be useful to the overall effectiveness of the global supply chain.

2. How can private sector advances in blockchain for supply chain management be leveraged by the government, either to improve interactions with the private sector or to re-engineer government processes?

Answer: The GTD Platform is a private sector advance in blockchain for supply chain management. By creating a secure, immutable, central location for documentation and real-time visibility into supply chain events the platform could help the government in multiple ways. First, by maintaining previously disparate, siloed data in one place the centralized blockchain solution will provide structure around which the government could re-engineer its processes. The platform's structure could also drive new means of interacting amongst all supply chain participants, to simplify the process by which one participant can gain necessary information from another (whereas such information exchanges have up to now been complicated by the disparate array of systems and communication methods amongst supply chain participants). For example, we've heard from another US government entity that it does not currently have global visibility to ensure governmental funded contracts (both military and civilian) are moving on US Flagged vessels as required by law, especially when shipments move through transshipped ports and when a freight forwarder (vs the ocean carrier) handles the bookings. Having the GTD solution, with the capability of following a US Flagged vessel and its cargo from end-to-end would provide a solution, saving time and manual labor costs in the process.

Responses by Mr. Chris Rubio

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

“Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods”

Mr. Christopher Rubio, Vice President of Global Customs Brokerage Staff, United Parcel Service

Questions Submitted by Ranking Member Daniel Lipinski,
Subcommittee on Research & Technology,
House Committee on Science, Space, and Technology

1. What potential do you see for blockchain technology to improve government supply chains, keeping in mind that the government delivers many “products” such as services, data, and tangible things, that have long supply chains? How can private sector advances in blockchain for supply chain management be leveraged by the government, either to improve interactions with the private sector or to re-engineer government processes?

Answer: Just as blockchain can help improve private sector supply chains, this technology can be harnessed to improve public sector supply chains as well. From social security to submarines, blockchain holds the potential to help streamline and secure government procedures and data. This technology may be ideal for the U.S. government as many of its processes have “many parties, many rules, many steps [...] and a critical need for very high levels of privacy protection and security from breaches.”¹ In addition, customs enforcement is one area where blockchain can greatly improve interactions between the government and private sector. Blockchain could enable greater transparency of a transaction, possibly including what’s in the box and who’s buying it, how much they are paying for it, assurance that duties and taxes are paid, and possible confirmation that shipments are not under-declared—resulting in faster release and a more trustworthy product supply chain. This not only helps the U.S. government ensure that only legal products enter the country with the proper duties paid, but it also greatly benefits UPS customers big and small as their items will spend less time in customs. All told, the U.S. government can harness the power of blockchain to improve its supply chains, akin to what the private sector is beginning to do.

¹ <https://longitudes.ups.com/how-businesses-and-governments-can-capitalize-on-blockchain/>



COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
May 8, 2018

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

Statement by Chairwoman Barbara Comstock (R-Va.)

Leveraging Blockchain Technology to Improve Supply Chain Management and Combat Counterfeit Goods

Chairwoman Comstock: In February, we heard from witnesses about the non-bitcoin applications of blockchain technology during a joint hearing. While we learned much from that panel, it became evident that there are many more potential applications of this technology to examine. Today we delve into some of the potential and proven applications of this ledger technology, namely in the areas of shipping, logistics and customs.

The global marketplace has added complexity to modern supply chains and complicated their effective management. The supply chain of a given product can span several stages and geographical locations.

Modern supply chains typically consist of several individuals and entities, involve multiple payments and invoices and can take months for a product to move from beginning to end.

As manufacturing becomes increasingly more globalized in nature, managing modern supply chains will become increasingly complex.

While this has implications for the speed, efficiency and accuracy of goods ordered, a larger concern is the authenticity of an ordered item as counterfeit products increasingly saturate the modern consumer market.

According to one of our witnesses today, each year, more than \$16 trillion worth of products cross international borders. Yet by some accounts, counterfeit and pirated goods are expected to siphon \$4.2 trillion from the global economy by 2022.

Despite living in an age where we can have almost anything delivered in 24 hours—or less—we still deal with such questions of accuracy and authenticity when it comes to the goods ordered.

It's a side effect of having access to an international supply chain as we can never be quite sure of the origin of the product purchased.

Today's hearing will provide some insight on how blockchain technology may help tilt the scales in favor of the consumer with better tracking and transparency of the supply chain.

Maersk for example, represented at our hearing today, began a collaboration with IBM earlier this year to digitize the global supply chain.

A few months ago UPS, also represented today, announced it would join the Blockchain in Transport Alliance. The alliance provides a "forum for the development of blockchain technology standards and education for the freight industry," with hopes of jumpstarting standards development for the shipping industry by implementing a secure blockchain system.

Even the federal government is involved as we will hear about programs within the Department of Homeland Security's Science and Technology Directorate relative to blockchain technology.

I hope these efforts will prove fruitful. When consumers are faced with a deal that seems too good to be true, they should feel confident to have found a deal that is a bargain and not a counterfeit product.

###

