

National Security in the Age of the Blockchain
*A Conversation with Yaya J. Fanusie, Kiran Raj, Tom Robinson, and Jamie Smith,
moderated by Juan Zarate*

ZARATE: Good afternoon everybody. Welcome to the Center on Sanctions and Illicit Finance here at the Foundation for Defense of Democracies. My name is Juan Zarate. I'm the chairman of CSIF as we affectionately call the Center. I'm the senior counselor to FDD, also sit on the board of advisors to Coinbase.

I'm honored to be here today. Thank you so much for coming. It's a great crowd. We saw the RSVP list, a really diverse set of backgrounds from government to industry to technology to media all gathered together. Let's go over some ground rules before we get into the discussion.

First, if you could silence or shut off your cellphones or iPads, that would be very helpful. This will be live streamed. We're live now so be on your best behavior. We'll reserve the last half hour of the program for Q&A, so think about the questions you may ask based on the conversation or questions you've had walking in the door. Try to refine them if possible, and we'll get to your questions. We'll ask you to identify yourself obviously at that point. But with that, why don't we start. And again, welcome here to CSIF.

There's no dearth of attention to the issues related to digital currency, blockchain technologies, or the digital economy. One need only read the newspapers or listen to podcasts to know that there's intense interest in this space. The Washington Post today had a piece on Bitcoin and what this means to libertarian ethos. There's reporting today of IBM and Maersk launching a blockchain technology firm for smart contract and logistics tracking. And of course, we've seen the flurry of initial coin offerings to the tune of billions of dollars this past year fuel lots of attention in the space.

What we want to do is bring light to this discussion, and I'm very proud that at CSIF, what we've done is try to drive cutting edge analysis around these issues. Not just where the risks lie in the space of the digital economy, the use of blockchain technologies or even new digital currencies, but also the opportunities. Opportunities for greater investment efficiencies, and even greater clarity and traceability in the national security and law enforcement space.

I'm going to with pride, wave around two of the reports that we've issued. One last year in July by Michael Hsieh and Samantha Ravich on Leveraging Blockchain Technology to Protect the National Security Industrial Base from Supply Chain Attacks. I commend that to you. And then just last week, authored by Yaya Fanusie and Tom Robinson, the report Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services. A really fantastic paper on looking at illicit financing flows using set data sets that Elliptic provided CSIF.

It's real-world analysis that isn't just speculative. It looks at trends and patterns and we're going to talk a little bit about that today. I'm very proud of the fact that CSIF's doing this work, and hopefully this conversation furthers our collective understanding of the space and where we're headed from here.

With that, let me introduce the panelists. These are four great professionals in this space who've done work in their own right in the research space. Some in government, and now certainly in industry. Starting at my far right is Yaya Fanusie. Many of you know Yaya as the Director of Analysis for FDD's CSIF. He's a former econ and counter-terrorism analyst at the CIA. Yaya and I got a chance to work together when he was in the IC, and Yaya's always done remarkable work and continues to lead our efforts in this regard.

To my immediate right is Dr. Tom Robinson. Tom and Yaya authored the report I just mentioned. Tom is the Chief Data Officer and co-founder of Elliptic and Tom will tell us a little bit more about Elliptic in a second. He's done a lot of work advising government tax authorities and regulators on cryptocurrencies. We'll talk a bit about where the regulatory environment's headed with Tom's help.

To his right is Kiran Raj, the Chief Strategy Officer for Bittrex, a very important digital currency exchange. He is the former Deputy General Counsel at the US Department of Homeland Security, and he's worked at the intersection of technology and law enforcement for nearly two decades. He and John Roth, now also at Bittrex, wrote a really interesting piece recently on the need for national security professionals to get involved in and bring attention to this space. We're very proud to have Kiran here.

And last but not least, Mrs. Jamie Smith. Jamie's a pro in this space. She's the Global Chief Communications Officer for the Bitfury Group. She's also the CEO of the Global Blockchain Business Council. She's leading efforts globally on bringing regulators and industry together. She has extensive experience in government. She was special assistant to President Obama, held senior positions in the Office of the Director of National Intelligence, and also on Capitol Hill.

As you can see, we have a great mix of experience and backgrounds for this discussion. So, let's do this with the discussion; we're going to divide this into three parts. The first part is, let's set the baseline for our understanding of both the technology and where there's an evolution in the industry and the thinking about what the technology brings.

The second part of the discussion, we want to focus on the risks and opportunities that the panelists see. And then finally, we want to dig a little bit deeper on the national security implications. Not just with respect to money laundering and countering the financing of terrorism, but also the use of these technologies by nation states either to evade sanctions, financial regulation, or even to undermine the US dollar or the US-based financial system.

So with that, let me start—Maybe Jamie, let's start with you. Can you give us a bit of a primer on what blockchain technology is, how that relates to digital currencies, and how you see the environment evolving?

SMITH: Happy to. I should also mention that I was at home with my 10 day old baby when a friend of mine who used to work at the White House in the Office of Science and Technology Policy who left to go to MIT to study this technology called me and said, “Hey, I think you should leave your really safe job with two small babies and go into this really cool

space of Bitcoin.” This was two and a half years ago and I said something along the lines of, “Are you high?”

I said, “That’s criminal money. I don’t want everything to do with that. There’s no way.” And he said, “Well, that’s the problem. That’s what people think.” I say that because I went through the arc of understanding this and I think a lot of people in this room and those who you know were going through as well. And so, my understanding of this technology came very organically. I was mostly self-taught with a great team of experts that I could lean on to ask a bunch of questions over a course of about three months on my maternity leave. Then I dove off this cliff and went into this space and no regrets looking back. It’s been really exciting.

The way that I think of this is like a train track between you and me, or you and me, or you and me, and you want me to send you an asset. That train track you should think of as the blockchain. It is a mechanism by which you and I can send an asset to each other. The car on top of that train track is a digital token. And because if I’m going to send you \$1,000, I need to attach it to something. It needs to have that data point where I can say, “Okay, now I just sent it to you.” And it needs to be recorded on some sort of system.

That system that records it again, a blockchain. The digital token, the most famous one is Bitcoin, but there are actually many. I think 200. There’s actually I think even more and growing. Those are called cryptocurrencies. The reason that they’re so interesting from regulatory standpoint is because what I did is, I attached \$1,000 and I sent it to this nice lady on the blockchain, attaching it to the Bitcoin and I sent it to you.

Now, the question is, does it really just have to be money? Of course not, it could be any asset. It could be music, it could be a movie, it could be a piece of my identity. It could be electronic health record. And so of course, what makes this so fascinating is the simple concept—Sorry, what makes this so fascinating is the simple notion that not only from a regulatory perspective are you potentially regulating currency, but you’re also regulating all sorts of assets. That makes this space not only green, but sort of fluorescent green. And then just to top it all off, the actual token has a value. That is sort of blowing everybody’s mind and really raises a lot of important questions.

The last thing that I will mention and I don’t want to get into all of the inner workings of the security, but it’s important that you understand the evolution. When the internet was created, it was created to move information and it did that. It did it phenomenally and it changed the world. But what nobody could actually figure out how to do is to move an asset securely. And so, a bunch of geniuses came up with the pretty simple idea actually of saying, okay, well, all of this information is currently stored in a silo. That silo is pretty hard to break into, but it’s not impossible, and once you break in, it’s party time.

So what we’re seeing are Equifax, Nasdaq you name it, big, big hacks. So a bunch of geniuses basically said, “Why don’t we take all the data that’s in these silos and break it up into thousands of pieces and put it all over the world?” So instead of breaking into a house, you now have to break into an entire city. And in order to do that, you have to break into every single

house all at the same time and it makes it a whole lot harder. So, you'll often hear blockchain technology described as distributed ledger technology, which is synonymous.

Distributed ledger technology just means we've distributed it all over the world and that is really important because, I'm not saying it's un-hackable, but it's a whole lot more difficult to hack. And every 10 minutes, a new house is built. The Bitcoin blockchain is 10 years old, no one's been able to hack it and every 10 minutes, we're building a new block in the chain of blockchain.

I know that was very brief, but happy to answer more questions. But I think it just gives you hopefully a little bit of a sense of why this is so multi-layered, exciting, risky, interesting, promising, et cetera.

ZARATE: It was very helpful, in part because the divide between understanding the rails and what sits on it is really important. I remember just five years ago sitting with some major global banks where the discussion of any element of the technology was met with an allergic reaction because it was the assumption that what you had to talk about was Bitcoin. The thing that was in the back of everybody's mind was Silk Road, Liberty Reserve, Mt Gox in terms of the stability. Not understanding quite clearly that we're talking about rails of the road. Now you have banks investing in these ideas quite aggressively. Kiran—

SMITH: Well, if I may.

ZARATE: Yeah.

SMITH: There's two things that I really had to understand when I started in this space for those of you who are new that I would recommend. One, there are a lot of people in this space who think of this as kind of that next wave of the internet. What I said to a lot of people who I think have invested in both the original internet and this, if you want me to believe that, then what year is it at this point? It's hard to find people, and maybe this panel will disagree, who go past about 1994.

So, I just want to kind of level set. When you're learning about this, you are really at the forefront of learning about this. Google didn't happen till what, 98? We didn't have Facebook till 2007, so it's very, very early in this stage. I'll just leave it there. It's very early.

ZARATE: Kiran, maybe if you can elaborate a little bit more on the technology itself, how you see it evolving and the explosion of interest in recent months. And in particular, Jamie's point about not just needing one type of digital currency but, you could send contracts for example securely on a blockchain. Can you explain that a little bit and what you're seeing in the marketplace?

RAJ: Sure, happy to do that. The company I work for Bittrex is a digital currency exchange. Unlike a lot of exchanges, certainly in the United States, we actually have a number of different of these digital tokens on the exchange. The reason for that is, we see the industry. It

started off with Bitcoin and then there was a few other coins after that, but there's been an explosion in these different types of blockchains.

Blockchains are, essentially to use Jamie's analogy like the rails. And if you think about Bitcoin, it's old rickety one because it was the first one ever built but everybody knows it and everybody wants to ride on top of that rail. But there's actually a lot of new rails and a lot of new ones that are being built every day that have a lot of interesting features on top of it.

Smart contracts is one that is normally associated with the Ethereum blockchain that a lot of people have heard about. But there are so many more out there and every day, more and more people are innovating and they're building new blockchains that can do a lot of interesting things, more than just digital currencies. So, digital currency is in many ways the first vertical, the financial space. But there's a lot of interesting applications out there.

One example is you know blog content. There's a lot of regimes out there that want to censor people from putting blogs that might be critical of a particular government. So, there's actually a digital token out there that you can buy that will actually help you post blog content in these regimes that would otherwise take down the blogs. We're seeing a lot of really interesting applications being built on these different types of blockchain technology.

To use the internet analogy I think is a really good one because I do see blockchain technology as being transformative the way the internet was, but we have no idea who the winner is going to be. We have no idea if it's going to be Bitcoin or Ethereum or one of these other blockchains that people are building now or have yet to be built. And that's sort of the really interesting part of digital exchanges, in some of these marketplaces where you allow the free market to decide who's going to win because of the feature sets and all these other interesting applications that you can build on top of the blockchain.

ZARATE: Let me ask you this and this is, to be honest, I'm here to learn just as much as many of you. Help us understand, you have different consortia trying to create blockchain systems or ecosystems. Some sort of closed-loop, some more open. Can you explain how that works in relation to what is the open system, the open ledger system, that Bitcoin's relied upon. For example, I mentioned this IBM-Maersk shipping line consortium or new company. Can you create closed-system blockchain systems within particular units or particular institutions?

RAJ: Yeah, you definitely can. There are such things as private blockchains. One of the interesting things about blockchains is, it really is—Public ledger is a good way to think about or distribute ledger technology. But I think sometimes people just add blockchain to something just because it's a good word to use where in fact for a lot of private transactions, you can just use a database. You don't actually need blockchain technology.

Where a blockchain actually has most of its value is when you want to have something be public and secure. That's its core functionality, so for a lot of these, I would say marketing statement, I don't mean the one that you're talking about, but just generally. You can see a lot of marketing out there of people getting into blockchain. But, unless you have a really good application and use case where you need it to be able to be distributed across in a public way and

securely, that's really where blockchain technology comes in rather than a lot of the private-to-private situations that you see out there.

ZARATE: Tom, can you speak to first of all, the work that you and your company do, but also the mechanics of how people operate within the digital currency space and with blockchain technology?

ROBINSON: Sure. At Elliptic, we look to identify—Sorry, identify and reduce the illicit use of cryptocurrencies. We are going to talk I think today a lot about the illicit use. I don't want to make it seem as though that's all Bitcoin is used for, but it's certainly a risk. Every means a value transfer can be used for criminal purposes, but I think Bitcoin is in some ways particularly suited to it for a few key reasons.

First of all, it is censorship-resistant so the distributed nature of the network means that there's no financial intermediaries who can block a payment or prevent a payment from happening. Secondly, it's digital, so basically, we now have value as data. Any way that you can store data or transmit data, you can now do the same with value, which means you can now send arbitrary amounts of value across the world, across borders at the click of a button like sending an email. And the third reason is because it is perceived to have at least some level of anonymity.

It's not actually true to say that Bitcoin is anonymous because Bitcoin is based on a blockchain and the blockchain is a list of all transactions that take place in Bitcoin. It says, "Two Bitcoins went from address A to address B." What you don't have though, is any concept of identity. You don't know who is making these transactions and that's the problem.

So at Elliptic, we work to tie identities to those Bitcoin addresses in order to build up a picture of who is transacting with whom. We use that capability for two types of customer. First of all, law enforcement agencies who are looking to trace Bitcoin payments and identify who is transacting, we help them with that.

Secondly, we help Bitcoin exchanges and other financial institutions to fulfill their anti-money laundering requirements. They want to know that if they're receiving Bitcoins from their clients, did that come from a legitimate source or did it come straight from ransomware? So, we provide them with software that lets them screen those transactions for risk.

ZARATE: Perfect. Yaya, let me ask you a little bit more about this in terms of the research you've done and start to get into some of risks. I also want to ask the whole panel a question about utility given value of digital currencies and all the speculation that has swirled around that, as well as issues of volume. It's a big technical question as to whether or not major transactions globally can actually sit on blockchain in mass and at the speed and without friction that most would want. Anyway, Yaya I want you to get into some of the research and things you've seen, but I also want to get into some of these other technical questions.

FANUSIE: Yeah. I'll probably start by saying, once you get into blockchain and cryptocurrencies, people talk about the rabbit hole. There's definitely an arc that comes from researching this. Usually starts out, let's say—Before the arc starts out it's, "Blockchain, who

cares?” I’m telling you where I started from. Even doing illicit finance research before I was really looking at digital currencies, you know, “Why should I care?”

Then you go through the stage of, “Wow! This stuff is amazing. Blockchain can do everything.” That’s sort of the second stage. It actually takes time. As you learn more about it, you look at the industry, you see the developments, you see what’s happening, then you get to I think the stage of realization of, “Oh, wait a second, a lot of this is still experimental.” You also do notice, you look at the industry you see there’s a lot of hype, there’s a lot of press releases which get reported as news.

People say, “They can do X, Y, Z. Blockchain can do this and do that.” Then you sort of look behind the curtain and you’re like, “Oh, well maybe in a few years,” or, “They’re just barely testing it out. They have four nodes and that’s supposed to represent what they think is going to happen.” So, I think we’ve gone through as an organization an evolution in terms of understanding the technology.

What I will say I think is important that we’ve come to with our research is blockchain technology is a new ecosystem. From an anti-money laundering or counter-illicit-finance perspective, we’ve I think discovered that to evaluate digital currencies or the Bitcoin blockchain, you have to get in your mind that you are looking at a new system separate from fiat currency.

And a lot of the rules that, or the paradigm that you have in looking at anti-money laundering in the regular conventional banking space, a lot of those assumptions—Some of them are fine, but there are some differences. So, one of the things I think that we’ve come to is, understanding that the digital, this decentralization ecosystem requires an understanding of different techniques. It requires an understanding of different types of entities within this ecosystem.

In our research, we looked and we could see what mixers are and what online gambling sites accept cryptocurrency. What are their features? What are they doing? How do illicit funds transmit through them and to them? So, it’s really I think—You get to a point of realizing we’re at a point of discovery. This is still early. Even in terms of answering the regulatory questions, we’re just beginning to understand what this ecosystem is, how it works. And then to throw a wrench in our understanding, we also realize this ecosystem is changing underneath our nose as we speak.

So, a lot of what we think about in terms of how do we deal with the illicit activity, we have to take into consideration that in a month, six months, 18 months from now, the technology could be very different in terms of its application. So, it’s a bit of a learning process in terms of looking at it, but I think we’ve been for the past several months doing more and more work, which you pointed to.

ZARATE: Before we go on, Yaya I wanted to come back to the point you made about the different actors in the ecosystem. Can you explain a little bit to the audience what those actors are because you’ve got wallets, you’ve got exchanges, you’ve got the mixers, you’ve got those

online casinos, et cetera, that leverage some of this? Can you explain that ecosystem? Maybe you and Tom can give us a quick snapshot on the conclusions coming from your research.

FANUSIE: I'll say one thing and then maybe pass it to Tom in terms of our research. We sort of separated our research. If you're looking at the Bitcoin blockchain, you have addresses and transactions as Jamie mentioned go from address to address. Maybe you can talk more about wallets, but what we looked at, we were thinking about, okay, if you have an address associated with let's say a darknet market like AlphaBay or something, where does that value go?

So, you have the entity and we could say AlphaBay, a darknet market trading in all types of illicit goods and illicit services, is an illicit entity. We can see the addresses associated with that market. We can see them in the blockchain. We know this because of past history or whatever is connected to that market. But then, we could also see what happens when someone purchases something from that illicit—gets Bitcoin from that illicit actor, and then takes it to some other platform.

We looked at the platforms that we call conversion services. Conversion services are basically platforms where people will go to cash out their Bitcoin or to hold their Bitcoin or to have wallets. We looked at different types of conversion services. Some of them were mixers, which would just receive Bitcoin and then mix them up in a way that you can't see where that Bitcoin has come from.

You have what most of us know about, Bitcoin exchanges, which I'm sure you all can talk about. Those are where people who have accounts, and the exchange is really the custodian of your Bitcoin. You can see on the blockchain, this Bitcoin came from AlphaBay, it went to this exchange, and there's a trail there that you can audit. We were looking at illicit activity as it moves to a conversion service because we had to provide some narrow parameters just to figure out, how are funds moving? How are illicit funds moving? That's what we tried to do with our report.

ROBINSON: We saw that the conversion services with the greatest exposure to illicit Bitcoins were the mixers in the gambling services. A mixer is an online service, usually run on the dark web, usually completely anonymous where, as Yaya said, can deposit your Bitcoins and receive different Bitcoins back.

That's helpful because as I said, the Bitcoin exchanges are screening all of their deposits to see where the Bitcoins came from. If they saw it's come from a dark marketplace, they will take appropriate action. But if a mixer has been used, it makes it much more difficult to trace those coins back to their ultimate source. That's why mixers are used.

ZARATE: Fascinating. Jamie and Kiran, let me ask you, how are regulators dealing with these challenges? The challenges of perceived and real anonymity? The fact that you have had illicit actors leveraging this? The fact that Bitcoin is preferred in a lot of the ransomware cases that have been made public? How do you see the regulatory environment shifting and evolving and anything on the horizon that you see from a regulatory standpoint given the outreach that you all do?

SMITH: I would say it's very different around the world. One of the things that was very eye opening for me as I sort of went into the real world post government, got my real jobs, was, I did not quite understand the animosity that exists in certain pockets of the world towards the United States for being so domineering in the tech space. There are a lot of people in the world who believe that this is their chance, that this blockchain crypto space is their chance to emerge whether you are in Hong Kong or Brussels or wherever, London, et cetera.

What shocked me was that when I walk around DC and I—this was two years ago, but hasn't changed that much though this room is bigger. You still a lot of people who say, "I don't know what you're talking about." If you to an event in Hong Kong or in Beijing, which we've done through the Global Blockchain Business Council only a year ago, there were 5,000 people there and over 30 regulators, who were all on stage talking about this technology.

If you go to London and you say blockchain, it'd be hard to find people who don't know what you're talking about. I am severely heard about the US angle on this. I think we are asleep at the wheel. I think this is moving way faster than people understand. And while it's nice that we're all learning, we need to learn really quickly and actually get ahead of this. Because while what we're talking about is really interesting. There's actually major, big dynamic forces at work here.

You have a lot of opportunity, but you also have a lot of countries who are looking to use this to affect the dollar and affect our security and our ability to navigate this new tech space. So, it concerns me greatly that there are in my mind way too many regulators in the US government who are just waking up to this and they're still in this mode of, "Oh Bitcoin, it's like this..." I mean, there's so much more to this and it's just time to get this moving a lot quicker or I think that we're just either from an economic standpoint, they're just going to pass us by and from a national security standpoint, we're going to be constantly chasing what's happening in this ecosystem.

ZARATE: Kiran, what do you think about that?

RAJ: I guess I see two big trends that I think regulators need to keep in mind as they're trying to learn more about this space. The first one is centralization versus decentralization as we sort of talked about a little bit already. Exchanges are places where everyone can go and you can trade different digital tokens or digital assets with each other. And because of the way exchanges are built, the exchange can identify everybody on the platform that's doing the exchange.

But there's actually out there a totally different mechanism like a decentralized type of an exchange where because of the way the technology works, where I can send you my Bitcoin just between you and me and we don't have to have anybody in the middle. There's actually software programs that are being built out there. Algorithms to facilitate those type of transactions, even if I don't know who you are. Those are completely decentralized types of transactions and those are very difficult for national security professionals, law enforcement, and other folks who are trying to fall the illicit finances to track because there's no way to really identify who's on either side of the transaction.

So, there's a big fight now between those of us who want more of that centralization where you can identify who are the users of the system versus those who want the more decentralized. I think regulators have to be careful, depending on the actions that they take whether they're moving people over into a decentralized world rather than a centralized world. That's one big piece, one trend.

And the other one is the one that Jamie mentioned, it's the US versus international. One of the things that we see is, a lot of the regulators in the United States trying to think, "How do I get my hands around these issues? How do I get my hands around these problems?" Because, it is a new space and a lot of the existing regulatory framework doesn't map quite well on to the digital assets and digital tokens.

The problem that we have though is that because it's a truly global environment, anything that's done in the US, especially regulatory uncertainty, pushes people overseas to all these countries that are offering regulatory sandboxes, enormous tax breaks, all these other incentives, precisely actually for the reason that Jamie mentioned: they want to win this time. They lost the internet right? The United States has the biggest internet companies out there because we allowed the development of the internet, the innovation on the internet and I think a lot of countries see the blockchain as the next internet and they want to win.

That's something that I think regulators need to keep in mind because frankly, the more companies we have in the United States who want to do the right thing and want to follow the rules, the better we'll all be because you can identify the people who are doing it and root out the bad actors.

ZARATE: Tom, how do you see this from your perspective both from your UK perspective and given your industry work?

ROBINSON: US regulators were very quick to move on this. FinCEN issued guidance I think back in 2013 about Bitcoin exchanges being money service businesses. There's been state regulation, so the bit license in New York. I think what our research uncovered was that was probably a good move from an anti-money laundry point of view because what we saw was that most of the proceeds of crime in Bitcoin were being funneled towards Europe Bitcoin exchanges. We hypothesized that that was because there was basically no anti-money laundering controls on Bitcoin exchanges in Europe at the moment.

They don't need to do KYC. They do need to keep transaction records and for that reason, the criminals were going to those exchanges. That is going to change now. The fifth anti-money laundering directive, which will hopefully coming into force fairly soon does bring Bitcoin exchanges and custodial wallet providers within AML legislations. They will now have to do those KYC—

ZARATE: Know your customer rules, transaction-monitoring and screening all the dimensions of that regulatory regime.

ROBINSON: Yup.

ZARATE: Yaya, let me ask you a question because I several years ago had a radio debate with the founder of Dark Wallet. One of the interesting statements he made was, “Look, we want to kind of break the system and we’re okay with whatever uses of the technology are out there. Money laundering, illicit transactions, whatever.”

SMITH: I got to look that interview up.

ZARATE: It was a fun interview. I sounded like the grumpy old man I think in the interview. But in any event, one of the points I made in the interview—and I still believe this but I want to test this with you given your research and work—if Dark Wallet is the technology of choice for those seeking to evade the system, it in essence creates a regulatory and law enforcement intelligence target on the users of that system.

In fact, I argued even just saying that we're trying to facilitate money laundering gives the US Treasury Department the ability to use something like Section 311 to say that’s a primary money laundering concern and any transactions that touch Dark Wallet or anything in this ecosystem is inherently suspect and subject of regulation and scrutiny and hopefully law enforcement intel scrutiny.

That's a long winded way of asking, especially given your research, isn't there a tendency to collectivize some of the illicit activity in the ecosystem at least now, even though this is an open and distributed system? Aren't we seeing certain types of currency, certain types of transactions, certain types of mixers that are preferred in the illicit context? Is that a correct assessment?

FANUSIE: I think so, and you said something about, it's an open system. The interesting thing is that open system creates really a great form of raw intelligence. That's what I'd call it. The change here, and I think there has to be—there is some maturation that is happening within the crypto community and folks who maybe for years were saying what you're saying. I think we're seeing more of the realization now that if you want to survive as a business, it's going to be very difficult to take the stance that I guess Dark Wallet or that person had.

The other thing though which is interesting, which I think we've come to see, I've come to see the past several months is that what's now happening is that anti-money laundering does not have to be something that's just within the realm of compliance officers and law enforcement. This is what's brand new. In the old way, the legacy system, who does compliance and who does enforcement or who is privy to transactions? It's the folks who can get the banks to provide data or receive suspicious activity reports right? Most of folks in this audience, if you're not working with Treasury or FinCEN, you can't you can't look at suspicious banking activity.

So that has been the realm of law enforcement. But what do we have now? I think the Dark Wallet folks didn't realize this, now you have an opportunity where anyone can see this raw intelligence. As a former intel officer, raw intelligence is not the end all, be all. Raw intelligence, you still need analysis. There's still other due diligence that has to happen, but just the fact that this data exists provides an opportunity for investigation, for law enforcement. It really just is an investigators dream to see this.

And I think yes, the result of that is that it should be clearer now where illicit activity is happening. Because in an open system, yes there are mixers and there are ways to try to obfuscate your identity, but the fact that there's still a trail makes a strong case for being able to identify, categorize, which is what some of these tools are actually doing. So the new paradigm here is that anti-money laundering is something that others outside of the traditional centralized system can actually have a part of.

ZARATE: Tom, do you agree with that? Are there ways of even designing the rails of the system or even the technologies themselves to enhance transparency and traceability? Where is this heading?

ROBINSON: There are. Bitcoin is already pretty transparent. I guess you could also include real world identity in the blockchain as well to make it even more transparent. I think there is an emerging threat though of more anonymous cryptocurrencies, the likes of Monero and Zcash. In Bitcoin, you have a completely transparent blockchain. In Monero and Zcash, they're either obfuscated or completely encrypted, so you can't see anything about where the flows of funds are going to.

We're seeing a shift on the dark web towards use of these currencies. Shadow brokers now ask for payment, for their exploits to be paid in Zcash. We're seeing a number of dark marketplaces adopt Monero as well as ransomware adopting Monero. So, this is an area of concern for us. I think that regulators need to decide whether Bitcoin exchanges should be allowed to exchange currencies like that because I think they're fundamentally different in terms of their risk profile to something like Bitcoin.

ZARATE: And I think that is something that we haven't seen with the regulators, is the ability to both help industry and to understand themselves what's the risk rating around these technologies? They often get sort of lumped together and there isn't the nuanced view. I think that's in part—the analysis you've done it helps quite a bit in that regard.

ROBINSON: Yeah, so going back to the EU legislation, that actually refers to Bitcoin exchanges specifically. There's no understanding of the nuance and the fact that there are hundreds or maybe even thousands of different cryptocurrencies out there with different risk profiles.

SMITH: Well, in your Coinbase, which you're on the board of, they accept four coins right now. I don't know what process they're going through to decide that those are their favorite four coins but, they're the most established and it's just interesting, I mean, I looked to Coinbase to tell me a little bit, but I don't know that that's the path we need long term, is that companies are telling you what they've decided are the most legit. It would be nice to have a little bit more guidance from regulators who actually understand where they're rating, as you put it.

But it was in this very room actually, a round table that you put together whether a number of FBI agents or representatives who said that, "Look as interesting is this is, and we get it, we know this is so critical," I don't know what percentage they gave, but a very low percentage of people in the FBI are educated about this, understand it, and they don't have the

resources because they're too busy working on tracing other types of crimes. And so, I think regulators, particularly United States need to also allocate funds for additional resources so that people can get up to speed quickly.

ZARATE: I think it argues for and this—putting my old Department of Justice hat on and Treasury hat on—this argues for some task forces right?

SMITH: Yes, yes.

ZARATE: We've had HIFCA task forces, we've had HIDTA task forces to focus on particular vulnerabilities with respect to financial crime or other criminal activity where you put the right experts together in a way to look at issues and I think we're starting to see movement—

SMITH: I would say a task force, and I also think that it is in the interest of the United States government to have every agency running some sort of R&D. Whether it's HHS on electronic health records, the VA for the same, but there needs to be a little pilots happening so that we are testing the potential of this. We haven't touched on this in this room and it's a whole probably other session, but I actually think that the United States government or other major institutions need to start actually mining these currencies because if you're going to put skin in the game and you're going to actually put secure information in these public platforms, then you should have a financial interest in this space as well.

I know that that's a whole other discussion and mining is a whole other layer of discussing this and it's a terrible word. It really just securing the blockchain, but why would the Pentagon ever consider putting any information in a public blockchain if they weren't actually reaping some financial benefit from it?

ZARATE: That's interesting.

RAJ: And actually on that point, I have heard a lot of various different government agencies talking about how they want to put really sensitive information on the blockchain because everyone equates blockchain with security. But doing blockchain right is actually really difficult. It's not that easy to truly secure a blockchain. One of the things that we're seeing from a lot of different companies who are getting into this space is that the promise of it is pretty high and the opportunities are high, but it's also very difficult. There aren't many people who have the experience to be able to truly secure a bunch of blockchains because they are susceptible to a lot of different cyber type attacks.

SMITH: Yes, and that's why you have to be really careful of all these people selling blockchain like in red and purple and whatever. There's a lot of snake oil out there at this point.

ZARATE: What about the question I asked earlier which we didn't get to, which is sort of volume and volatility. How do blockchain technologies deal with the issue of volume? And then to Kiran a bit of your point, the volatility and even security issues?

RAJ: Volume, not well. I mean, really to do blockchains at scale and at speed, you really can't be writing to the blockchain. That's why centralized exchanges, at least for now, are places where most people go is because an exchange can help you do things at scale and at speed that you can't do by just writing to the blockchain.

Bitcoin is a good example. I think last week I saw that the transaction cost for writing to the Bitcoin blockchain was so much larger than if you just wanted to use like Western Union or MoneyGram to send money overseas. There are enormous transaction costs associated with writing to a blockchain, and they can only handle a certain number of transactions per second, which is pretty small compared to the number of total transactions that are occurring on any type of exchange like Coinbase or others. I think that's something that also people don't quite understand about the underlying technologies. That it's not quite there to handle things at very large volume.

ROBINSON: I would just say that, that is a design choice though. There's always a trade-off between security and cost, and Bitcoin has gone for a very high security and very high cost. I think it's aiming to be a high-value payment settlement system and I think that different cryptocurrencies will emerge for different types of payments. You might pay for your coffee with Litecoin, but pay for a house with Bitcoin. It's a trade-off.

FANUSIE: And also, Juan, if I could add, it also depends on the landscape, where you're operating because a lot of people point to the volatility issue here in the US and say, "Okay, why would you have ... Why would you use Bitcoin for X, Y, Z?" I was listening recently to the CEO of one Bitcoin-based company that does cross-border payments in Africa. The response of that company was, "Well, the volatility is better than what we deal with in Africa in terms of cross-border payments within Africa."

So for them, for that use case, it actually makes sense for them to use this sort of system. It might not make sense here in the US or in Europe, and what that means is, it's very important to understand that use case. Because, when we look at, "Well, where will this technology develop?" It's not going to develop where people have made the best cases and presentations for it. It's going to develop where there's an actual use case that makes financial sense, that fits with the environment, where there's infrastructure for it.

So we almost have to look outside of our present situation here in the US and identify, "Oh well, that state actor or the business sector in that country might actually benefit because for them it does make sense."

RAJ: And that's the answer to the question of why there are so many digital tokens out there, because there's an enormous number of use cases and a lot of people out there will build a token specific to a particular use case.

SMITH: Absolutely. I think there is a developed world discussion and a developing world discussion. I do think it is important—No one's challenged me on this stat, so I'm just going to keep running with it because it's based on a collection of stats. But I would say

somewhere in the range of 60% to 70% of the world's population are living under some pretty broken systems and they're pretty mad about it.

It's no coincidence that this whole blockchain based structure debuted in 2008. There are just people who are trying to start businesses and trying to move money and assets around the world and they don't work. Things don't work. It is so hard to sell your land or even to prove that you own that land. And there are a lot of use cases for this technology that we are seeing come to life all over pockets of the world.

ZARATE: Jamie to that point and what you were saying earlier, a lot of the use cases may emerge outside of the financial domain right? In terms of supply chain, shipping, contracts, et cetera.

SMITH: Yeah, I mean Walmart is using this technology to track meat in and out of the United States for the Country of Origin law. They have their own private blockchain but as you were saying about private blockchains, think of it like an intranet. I'm dating myself but, remember when we were like, "I don't know about that internet thing. I'm going to have my own right here, and then it's going to connect to Firefox," or whatever that was.

That's like private blockchains, but what they're going to eventually do and you're already seeing this is an anchor to public blockchains so that you get that extra security. But a private blockchain is just like a small town where it's still distributed and you're still verifying things through consensus, but it doesn't have that same level of security as a public blockchain because there aren't as many nodes. But it's more secure than a centralized silo of information that you can just break into.

So long way of saying that we're seeing so many cool things happening. I co-chair the World Economic Forum's Blockchain Council and my co-chair is the former president of Estonia because that was one of the first countries to do this type of work and why wouldn't they? They have real national security interest in trying something new, there is a big country to their east that is looking to tap into their systems, and they have nothing to lose. You're seeing a lot of countries saying, "Well, yeah. I'd like to try something new. If you're more secure and more efficient, let's roll."

ZARATE: Yeah. Before we go to the Q&A, and we're going to do that in just a minute, I did want to go back to this question of national security concerns beyond the use of digital currencies by illicit actors. This idea of other countries, especially those that are trying to displace the US system or challenge US authority, where those risks lie. Yaya, can you talk about that and anybody else who wants to comment on it because I think there's a very important dimension of the forward looking risks and potentially opportunities in this space.

FANUSIE: Absolutely, and I probably have to clarify because the way this often gets discussed and it usually gets discussed in relation to sanctions and people say, "Well, will Bitcoin or will a blockchain allow people to evade sanctions?"

ZARATE: Venezuela establishing Petro.

FANUSIE: Right, that's what's been happening. I'd say some of that is overstated, but there's an aspect that actually is understated that we need to think about. I think if sanctions evasion is using let's say a cryptocurrency that exists, Bitcoin, to pay a designated entity or designated person, will that happen? I'm sure it happens, it may happen in pockets. But I think that in the short term, the scope of that is limited. In order for there to be massive sanctions-evasion in that manner, you're probably still going to have to touch the traditional financial system.

SMITH: You've got to off-board it.

FANUSIE: To do sanctions evasion, what really works is front companies and there's a very well-established—I mean, North Korea, we can talk about North Korea—very well established at using shell companies and front companies to evade sanctions. So I think that's overstated. Bitcoin is not ready to enable North Korea to evade sanctions. But what I think is happening that we have to keep our mind on is sanctions resistance. This is where you see, whether it's Venezuela creating their own new currency, whether it's Russia really investing in blockchain systems, which it says they want these systems to replace the US banking system or the global system and the SWIFT system.

There's a strategic intent of there that I think is being telegraphed where the aim is not to evade sanctions tomorrow, but to create a system so that when there are sanctions, whether it's US sanctions, UN, EU sanctions, that the actors who are designated are resistant to it because they have an alternative means.

Now, the other part of that is, it's not so easy to happen. Again, this is I think a horizon issue. It's similar to having a social network like Facebook. Let's say you're kicked off Facebook and you say, “I'm going to do my own Facebook.” Easier said than done because of network effects. But the thing to keep in mind is, the way technology develops, I think we have to really be careful that we don't dismiss and overlook what is developing because they've been pretty clear, I mean, Russia, even China, in terms of trying to displace the dollar.

ROBINSON: Yaya, would you see those as centralized digital currencies as opposed to decentralized ones?

FANUSIE: That's the other thing. What a lot of these actors are doing is planning to create a currency that would be centralized, that would be a Russian “Bitcoin.” Venezuela is saying that it's going to do the same thing. That's actually a bit different than what we're seeing with decentralized currencies like Bitcoin.

SMITH: One thing I thought was—I think about this a lot. I was in the intelligence community for all of a year. I thought I'd be there the whole time, but when the White House calls you got to go. But three things happened while I was there. First we had WikiLeaks, then we had the start of the Arab Spring, then we had the Bin Laden raid. It was an exciting year.

But when I think about that year, what I think about most is that I think that the Arab Spring and WikiLeaks really started the beginning of this process of assessing our national

security threats in this open source world. We've always thought of our national security threats as secrets, these really big secrets. In fact, one of the first things that I was told and I can tell you this now because it's not really a secret was that the Nasdaq had been hacked.

Well, that wouldn't have been a secret in the national security world anymore. It just would have been in the news. Our ability to figure out how to assess what's happening in the open source world whether it's through Twitter, or Facebook, or social media, or now think of blockchain and public blockchains as like the social media of assets. There's so much public information and how do we as a nation and as a society assess all this information in a wildly strategic way? That is what I'm saying when I say we need to get on this because there is a lot of information moving and we're just going to have to go retroactively in looking at it. This is where I think the real analytics come into play.

ZARATE: Perfect. All right, let's open it up to questions. Great panel and again, I think we could talk for a couple of hours here. Why don't we start with the gentleman the back here with the sweater. And please identify yourself. Stand up if you could so people can see you.

TALLEY: Ian Talley, Wall Street Journal. I wanted to push a little bit more on the general undermining of the dollar. It seems to me that China got the Yuan Renminbi into the SDR as part of a legitimization prospect, and yet less than 1% of the global central banks hold the Renminbi. I think there's institutional reasons why they hold the dollar, so how could—Help me to understand how exactly a blockchain tech actually undermine that fundamental problem. Do you see what I'm saying?

Secondly, if I may, why would we not get a G7 OECD initiative like the BEPS Project where you push forward a regulatory structure where you include ID requirements, filtering requirements? And finally, does data sovereignty create some sort of issue where the distributed data is held? Who holds the key to access to the cloud data, et cetera? Yeah, let's leave it there.

ZARATE: Yaya, why don't you take the first one, Jamie the second, and Kiran maybe the third. And Tom weigh in as—no, no, you have to weigh in, you're not off the hook.

FANUSIE: Do you have a fourth question? I'll just say, and let me sort of—A caveat with my statement about states saying that they will use blockchain technology to displace or to displace US influence. Me stating that is not necessarily an evaluation on how successful they will be. In fact, my stance is, okay, easier said than done. Yeah I'm seeing statements, I'm seeing people, officials in Russia say that they want to do this. I am seeing pilot projects where there are banks which are saying by the US and the EU are piloting blockchain programs or blockchain experiments.

I think the vision and again, reporting almost their vision. The vision is that eventually, they will transfer to a system where their banks are linked to other banks around the world, but that they institute a system that is totally separate from the global banking system, based on the infrastructure of blockchain technology with the idea that to deal with their lack of capital, they could now transact with other parties using the same sort of blockchain system.

Now, there's not a name for it. We're talking about what's been happening in the past year that they've been investing in. It doesn't exist yet, but I think we're clearly seeing this intent, and we can see that it's based on, or it's a result of them trying to get away from our financial power and to distance themselves from it. So it's an evolving thing. I'm not sure how successful it would be, but I think strategically we have to look at it, evaluate it, and also coming from sort of an intel perspective, when you're strategically looking out at national security, you should be thinking about various scenarios, alternative futures, what could exist.

If this were to happen in the future, would we be prepared for it? How do we address that so that we're not short-sighted and myopia in how we deal with our national security? But I've never been on record saying, waving the flag, "Oh, this is going to end the power of sanctions next year." I don't think that's the case.

ZARATE: Yaya, we have read and I've articulated this, the concern about alliance of financial rogues and the ability of those that are excluded from the formal financial commercial system from collectivizing. The relationship between Venezuelan banks and Russian banks. The ability of Russia and China to give outlet to Belarus. The ability of these actors to interact and I think part of this is, is there an ability to use these new technologies as a skeleton for that sort of alliance and an alternate system? I think that's of concern.

Second thing I would say is, we've already seen this movement in the context of payment systems and credit cards. So, the Russians talking about their own national payment system like UnionPay to get out from under restrictions of Visa and Mastercard, which are then subject to US law. It's not an unusual trend. It's already being discussed, it's already happening, questions where these technologies emerge.

Jamie, do you want to handle the second question?

SMITH: Yes, but if I could just add one other thing. I said I wouldn't go into the whole mining thing, but it is really important to understand this in the context of your question. There's this word called mining and I don't know why they called it that because it sounds creepier than it is, but it is actually how this system works and it's very important that you understand. I didn't include it in my primer because it's a little more complicated. But at the end of the day, every 10 minutes, all of the transactions that are happening around the world on the Bitcoin blockchain get put in a block.

This is the space-agey part, so I just want to ask you to stretch your brain here a little bit. But all of these data centers around the world fight each other every 10 minutes to verify those transactions and they do it through the one language that everyone speaks, which is mathematics. Whoever solves the math problem, every 10 minutes wins 12.5 Bitcoin. Take out your calculators, that's a lot of money.

Now, when a Bitcoin's worth \$50, it's not that much money. When it's worth \$19,000, that's a lot of money. The largest amount of mining facilities, data centers that are doing this are at the foothills of the Himalayas in China. The other data centers are in other parts of the world. Some are great; Iceland, Norway et cetera—

ZARATE: Keep them cool right?

SMITH: Yeah, they got to be cold. But there are a lot of people looking into this mining space, especially with the hike in Bitcoin prices. But Ethereum has—People or mining these coins, so there is a financial incentive to both keeping the system secure, which is why it has such high levels of security, but there's also a financial incentive period. That is where you get into some really interesting dynamics. This is serious money going on and as you said, there's sort of a click.

On your other point, yes. There absolutely should be a big committee, a task force a, G7, G10, G20 discussion and I think that that's coming. I think there's no question. Some regulators have taken a little bit of a hands-off approach learning from the internet days of not jumping too quick, and I think that's wise, but I also think that time's coming for much more robust discussions of various rules of the road.

RAJ: And I guess on your question of where the data exists, it depends on what data you're talking about. If it's the public blockchain, that's accessible anywhere in the world. If you're talking about the identity of the users, it really depends on the system that you're describing, so for decentralized systems, potentially you don't have anybody who can identify a user.

From a US-centric perspective, there might be exchanges in certain jurisdictions where they're not open to getting US-processed. And of course, there's exchange in the US and other countries have MLATs or other things with the United States, where you can potentially get identities of users.

ZARATE: Next question. Young gentleman in the back.

MASSARO: Hi, Thank you. I'm Paul Massaro, anti-corruption advisor at the US Helsinki Commission on the Hill. I just wanted to thank you for the great conversation on specifically sanctions evasion. We're very interested in that, and I wanted a comment on that. Recently at a hearing that we had on the Magnitsky Act at five years, Bill Browder expressed his extreme concern about cryptocurrencies and the role they could play eventually in avoiding sanctions.

And economic adviser to Putin, Sergey Glazyev recently commented on the objective need that's—those were his words—for the development of cryptocurrencies, in order to evade sanctions. So, I think you really nailed it there with your idea of sanctions resistance. My understanding is, it's not at the point yet where it can really be used for effective sanctions evasion, but there is discussion in these sorts of states and it's pretty big.

With that in mind, we focused a lot on the regulatory structure today and how the agencies can catch up, but could you maybe comment and think a little bit about where and when it would be time to do a legislation on this? Can Congress play a role and that sort of thing? And then for my own knowledge just wrapping my head around this, if you don't mind let me ask a second question and that is, in a hypothetical where a state does develop a sort of national cryptocurrency of some sort, how would monetary policy work in that environment? Thank you.

ZARATE: We may reserve the second question for a different panel.

SMITH: Whole other panel.

ZARATE: So, let's take the first one very quickly. And I ask folks, let's keep it to one question.

FANUSIE: I'll just say very quickly, the legislation/regulation issue is tough and is interesting. The 2013 guidance from FinCEN I think was very good, as Tom pointed out. Bringing some certainty, raising up the standard level saying, "Hey, if you're going to do a cryptocurrency business, you have to fulfill these AML, KYC requirements."

One of the things that we're thinking about and we sort of allude to in our report is, there needs to be I think greater awareness by lawmakers, by regulators. That's been mentioned today. I think the idea of task forces or a task force, commission on digital currency preparedness, I sort of feel like we need to raise up the IQ level first on this currency because right now when you first get into it, you sort of think it is what you just heard and you really need to do a deeper dive.

I think regulators have been you know, some of them have been doing it, but I think across the board there is a need for more education. I would say that that's the first step. And assess what regulations don't apply, because the potential issue with launching too quickly is that the technology changes and we don't address what's happening next year.

ROBINSON: In terms of monetary policy, I think these would be centralized cryptocurrencies, they would be controlled by the central bank of whatever country, so they could have whatever monetary policy they want so they could issue new units anytime they wanted. I think this is one of the reasons why it would be very difficult to start one of these cryptocurrencies. Part of the reason that Bitcoin has value that has acceptance is that it isn't controlled by a central party. Gaining that same kind of acceptance for a centralized state cryptocurrency I think would be challenging.

ZARATE: Kiran you want to say something?

RAJ: The only thing I was going to mention about the task forces and committees I that I do think this is an area where it's very difficult for regulators to go it alone. To put on my old DHS hat, this is a perfect example of a public-private partnership opportunity where there's a lot of folks in the private sector who have a lot of experience in this area and want to work with the government, policy makers, regulators to help educate them on some of these issues. I think that's something we haven't quite talked about yet, but I think it's an important aspect.

SMITH: Can I just piggyback on that really quick to say also from a Hill perspective, it really is incumbent upon leaders on the Hill to understand that they cannot do this in one or two committees alone. The jurisdiction on this has to spread across many committees and that's why these task forces both in the executive branch, but also in the legislative branch are actually going to be so critical because they're talking about assets, these securities, commodities, currencies.

There's so many spaces that this stretches into and it's going to be really critical, otherwise you're going to have what happened with cybersecurity I think. I mean you had Senator Rockefeller introduced a bill and Senator Lieberman got really mad because he said he was guy in charge. They just fought about who was in charge for years.

ZARATE: In fact, I was testifying last week on sanctions issues before House Foreign Affairs and there was a commitment by the chairman based on concerns on these issues to hold a hearing on this issue. So it's great in terms of raising awareness but to your point, where are the hearing going to be held?

SMITH: Yeah.

ZARATE: Okay, next question. Let's go right here.

READ: I'm Russ Read, Circa News. I recently spoke with your colleague Emanuele Ottolenghi about the existence of Hezbollah and their illicit financial networks. We've spoken a great deal about states and what they may be trying to do, but I think we really haven't touched as much on non-state actors. What's the possibility of say a Jihadist group like Hezbollah or another using or creating perhaps even their own to facilitate their own transactions within their own sphere?

SMITH: 100%.

ZARATE: Yaya you can—

FANUSIE: Experimentation is happening. I think we've tracked over really the past year since last year a number of jihadist groups, jihadist networks, one trying to do fund raising using social media and putting up a Bitcoin address and saying, "Hey, donate to us." There is a group that we were looking at just a few weeks operating in Telegram Live. I haven't checked, but they might be operating to this day, seeking Bitcoin. They say they're located in Syria.

So we see this happening. Perhaps there's been an uptick because of the price rise and just now everyone knows about Bitcoin, but this is clearly a way to raise funds. Now, the thing I would say though is, there are lots of reasons why they have not been as successful as one might think. And just one, the difficulty of using Bitcoin. It's very easy to put up Bitcoin address, but it's more difficult to get people to widely adopt this as a fund raising method and there are lots of other alternative methods.

But absolutely, we should not—this is something that we've actually written a little bit about. There are clear cases of designated terrorist groups trying to raise money through Bitcoin.

SMITH: I'm sure there was some room just like this where they said, "What are the chances of ISIS or another group like it using Twitter to attract followers?" I mean, technology is just a tool. People are using it for various purposes. It is up to us to be smart enough to figure out ways to curtail that. This is a secure, immutable ledger of transactions. Surely we can find a way.

It's better than a bag of cash. We can actually figure out ways to trace this if we just wrap our minds around it and basically stop scratching our heads wondering what it is.

ZARATE: Tom?

ROBINSON: Yes, use of Bitcoin for fundraising, yes it's already happening. Will they create their own cryptocurrency? I think it's very unlikely. I don't think they need to, they can just use other open cryptocurrencies. And for the same reason, it's difficult for a state's actor to generate the community and the acceptance around a cryptocurrency, it'd be even harder for that kind of organization. I mean, what exchange would offer exchange services for that coin?

ZARATE: Next question. This gentleman right here, been very patient thank you.

GFOELLER: Mike Gfoeller, Council on Foreign Relations.

ZARATE: Wait for the mic just for folks who are watching online.

GFOELLER: Thank you. Mike Gfoeller, Council on Foreign Relations. We were talking about using Bitcoin for terrorist finance. That's an interesting point, thank you. But you were saying earlier that blockchains can be used to spread ideas, blog post and that sort of thing. Recently we saw how the Iranian authorities shut down the recent wave of protests in their country, essentially by shutting down platforms like WhatsApp and Telegram that were really popular and were used to organize demonstrations. Could frustrated Iranian opposition activists use blockchain technology to spread ideas and plan demonstrations? Is that technically feasible?

RAJ: There's definitely use cases out there, or tokens out there that would support that type of a use case. I don't know specifically if folks in Iran are using it, but just generally, yes that's a use case that is available. Even today that's available, and then as we move forward where more and more people are developing more innovative use cases, you'll probably see even more of that out there.

ROBINSON: There's a system called Bitmessage, which is very similar to Bitcoin except instead of transferring value, you're transferring messages. Completely decentralized, you can't take down any single actor and stop that system from working.

SMITH: If you think about it going back to the beginning, every transaction, if you wanted to break in and change the ledger, you'd have to break into every single house in the entire system and that is near impossible. So, when you're putting that content up there, a regime would really have to work hard, spend zillions of dollars, and have almost no return on that investment to change the record. That matters a lot.

If people are--think of polling. Think of going into Venezuela and asking people to text their vote on a phone, and if you stamped those results on a blockchain and the government says, "No, no, no, this is the results," and we say, "Actually, these are the results and you can't change them." There are housing ledgers that people are looking at. There are so many wonderful use cases.

There's also China has made mention that they would like to have a record of who's good and who's bad in their country. So that would be a bad use of this technology. Putting bad information on a secure immutable ledger is something we should all become very conscious of.

ZARATE: Next question right. Right here.

BIDWELL: Good afternoon. Chris Bidwell from Federation of American Scientists. Thank you all for a great presentation. Something that I lost though in the understanding is, I see in the news that Bitcoin or Ethereum goes up some days, goes down some days. What's driving that? And because it goes up or down some days, does make it make it valuable as a reserve currency for other countries in their reserve banks? Thank you.

ROBINSON: It's completely open market. There are various marketplaces all over the world where you can buy and sell cryptocurrency, so it just depends on supply and demand like any other foreign currency.

SMITH: There's a finite amount. You could break one Bitcoin up into zillions of pieces, but that the market is being driven. There have been big events that have happened. Korea established and made it a much more open possibility. Japan recognizes Bitcoin in a major way, and that took the price overall if you look at that moment from about \$2,000 to about \$12,000. I would say if India or another major economy decided to accept using Bitcoin, you'll see the price jump again.

But I actually think that what is lost in this is that each Bitcoin represents a high level of data integrity and data security, and in an Equifax world, that's worth a lot of money. The more people are realizing the security implications of these digital tokens and why putting information on them could be really useful, I think they're starting to see that, that could have quite a value. There are those who project that one Bitcoin over time, five, 10 years from now will be worth \$100,000 and even more than that because each one will house a tremendous amount of data.

ZARATE: Next question. Right here in front, and then we'll go here. Time for a couple more here.

MEIZLISH: Thank you, Max Meizlish from BGR Group. Earlier you mentioned the concept of an application called Bitmessage. If we're thinking in the preliminary stage of regulation versus something that is pseudo-anonymous, versus something that is more inherently anonymous, where do regulators strike the balance for that conversation? If you have a company like yourself that's working with law enforcement with pseudo anonymous platforms to track a chain, link it to an identity versus something that is more anonymous like a messaging app?

ROBINSON: I think that banks today have different policies depending on what kind of payment mechanism people are using. If you're looking to withdraw and deposit cash, there can be different limits than if you're doing a wire transfer. I think the same or probably the same for different cryptocurrencies. Already if you open an exchange account, you'll generally have a daily limit, the amount of Bitcoin you can withdraw a deposit. Maybe it's appropriate, that if you want to use Zcash or Monero, those limits are lower.

ZARATE: Question here?

MELIKYAN: Makar Melikyan, Embassy of Armenia. My question was, looking ahead like 10, 15 years, what this problem of Bitcoin file getting enormously big, what are the solutions for that? What is being discussed?

SMITH: With the Bitcoin file getting enormously big, what do you do about that?

ROBINSON: One argument is that storage costs simply go down faster than the Bitcoin blockchain size increases, so it's not an issue. There are some more technical ideas, which I don't fully understand, which will reduce the actual size of the blockchain but I think the general consensus is, it doesn't matter because storage costs are decreasing faster than the blockchain's increasing in size.

ZARATE: Sean, great to see you, welcome.

KANUCK: Good to see you , Juan. Sean Kanuck with IISS. Two questions, or actually the same question. The first being, how are the people who are actually setting this up, these different blockchain systems themselves, profiting? What's the profit model? And are they revealing the source code of these systems for external reverse engineering and penetration testing certainly from a law enforcement and other perspectives? So what's the profit model for the people setting these up that may reveal their intentions?

ROBINSON: Some cryptocurrencies have what is called pre-mine, so the founders of the cryptocurrency hold a certain amount of that cryptocurrency. They profit on the basis that the value of that currency will increase. Not all cryptocurrencies use that. Bitcoin didn't have that, but the early adopters again tend to have high holdings and therefore profit from the increasing value of cryptocurrency. I'm sorry, what was the second question?

KANUCK: Are they revealing the source code for external verification and testing?

ROBINSON: Yes, they're all completely open source.

ZARATE: Anybody else want to add on that?

SMITH: I think there's a lot of ways to make money. There's those who hold the actual tokens, that's the mining process. There will be an entirely separate panel on what are called ICOs, which is a whole new profit model that people came up with about six months ago. The SEC's weighed in a little bit, but I think everyone's been shocked by the uptick in that. And then there are consulting services frankly.

There's just a ton of companies out there and those are the ones that are both awesome and to be a little bit weary of who say, "Oh, we're providing services and we have blockchain capabilities." There's a lot of questions that one should ask to make sure that those are legit companies. And then of course the wallets and the exchanges are just like any other exchange.

RAJ: I think you see a lot in the token space. Sometimes the profit motive is incidental to the token. It's like they're trying to drive a particular use case, their own ecosystem and so the token actually, they don't make money off the token itself. It's driving people to their larger ecosystem is where they're going to make the money. So again, I think it just depends on the particular token at issue.

SMITH: Think of the token as like a share of an idea. People really either like the idea, or they don't like the idea. They'll buy the token and then if the idea grows, like if somebody came to me and said, "Blue Apron is my idea. Do you want to buy a token and invest in my idea," and I'm not a big VC or an institutional investor I say, "Okay, I'll buy 10 tokens at \$100." Let's say Blue Apron takes off, I just made myself some real money. If it doesn't, no harm no foul. Well, a little bit.

ZARATE: One last question. This gentleman, if we make it quick. Then I'm going to take the moderator's prerogative on the last question.

TENZING: Thanks. It's going to more of a remark. My name's Tenzing from DHS. It seems in our conversation, there's was bit of a contradiction because we're talking about how great the blockchain is and how it works and consensus, but at the same time we're talking regulation. Back to your analogy, imagine if the internet didn't have net neutrality back in the day. How far could the US have come in terms of that innovation? I'd love to hear your thoughts on that.

ROBINSON: I'd say that we're not talking about regulation of the technologies, we're talking about regulation of the services, which are the gateways that allow you to go in and out of these technologies. I don't think it is possible so regulate Bitcoin itself for example.

RAJ: And I think the type of regulation. We haven't really talked about that either, but it needs to be smart, it needs to be very targeted and trying to hit a very specific problem. I think if we do more overbearing type regulation and try to regulate the industry, especially in the United States is where you just get a ton of people leaving and moving offshore.

I think generally most people think that it makes sense to have some type of regulation, to make sure that there's rails and legitimate actors know where they can be in and that those who don't care about those rails like the person who might've been in on Juan's radio show, it's easy to identify who's on what side of the line.

SMITH: I cannot underscore enough what you just said which is that, any discussion of being able to stop this technology from evolving is useless. It is happening. It is game on, it's been 10 years. This train has so left the station, and it's just imperative that we actually start really understanding what's going on so we can both excel in it and do our best to stop as many bad actors as possible.

ZARATE: All right, let me take the last question and ask each of you. It's sort of a lightning round, will only last five minutes. What do you see is the greatest opportunity and

greatest risk when it comes to blockchain technologies and national security? An overarching way of ending the discussion. Yaya, let's start with you.

FANUSIE: I'll start, and I'll start with the greatest risk or threat, which has sort of been touched on. Maybe the thing that keeps me up at night, which is good in many ways because the technology provides censorship resistance. But as a former counter-terrorism analyst, I'm really concerned about decentralized media content. We all live in a world where if Al-Qaeda or ISIS puts up a video or a website, they have to go through a lot to keep that website up or to keep the content up, to keep the video—videos of be-headings right?

Because of our centralized system, it's difficult to do that. So censorship resistance is one of the strengths of the system, but from a counter-terrorism perspective or someone worried about that sort of propaganda, I'm concerned about how do we deal with that decentralized media that no one can take down?

The thing that I think I'm excited about is a term we haven't touched on, which is just crypto-economics in general. If we think about crypto-economics, the Bitcoin blockchain, what it allowed was, it incentivized people who didn't trust each other to keep the integrity of the system. I think one thing we haven't dealt with is, if we're thinking about what's the solution to the illicit risks of this technology, perhaps there's a decentralized way to incentivize through crypto-economics, through cryptographic computer science where you incentivize with financial incentives.

Maybe there are ways to decentralize good behavior on the system. You want your blockchain to be clean, maybe there's a way to come up with incentivizing a “clean blockchain.” Again, that's just sort of way out there, but I'm excited about the potential that this provides, even though we can't really see the solution yet, but I think it's something to really look forward to.

ZARATE: Jamie?

SMITH: Same answer for both, which is identity. From an opportunity angle, there are 2.5 billion, not million, billion people in the world who have no legal identity. They have no proof that they exist. Trafficking, human trafficking alone is gigantic. The cross border migration, refugees, terrorism, et cetera. If we had a system where we actually were able to log identities and have them be interoperable using blockchain systems where you could actually have them be through biometrics, I think that that could really be exciting and incredible and there's so much good that can be done with that.

I also have tremendous concerns with that and I'm sure we could spend hours talking about all of the different various risks, whether it's even possible. At the end of the day though, I think that these nonfinancial and even into the financial, obviously, of course, applications of this technology, if nobody—the big company that will emerge I think is the one who can truly establish identity because it's one thing for me to transfer my house to you, it's another thing for me to know that you are who you say you are. That to me is kind of the big white whale of this whole industry, is cracking the code on identity, but doing it in a responsible, ethical, and efficient way. Who knows, but it's big.

RAJ: For me the opportunity or risk are the sort of flip side of the same coin. From a risk perspective, it's that from a strategic US centric view, we will not have the next Amazon or Google. That I think is the biggest risk. The blockchain to me is the next internet and we are in this very interesting time right now where the decisions we make both in the private sector and the government will decide where that next Amazon and Google will come from.

On the opportunity side, I actually don't know what the next big thing is. No one really could see that Google was going to be as big as it was back in 1994 when the internet was just really starting to take off. So I actually think that that is the opportunity piece of this, which is that there are so many different use cases, so much innovation going on now that we want that to be here and that's the biggest opportunity.

ZARATE: All right, Tom?

ROBINSON: What concerns me is something I've already mentioned, but the more anonymous cryptocurrencies and their use by criminals. I think there's a big role here for regulators. These currencies will only be used if they're liquid, and so you need to target the exchange platforms where they liquidity exists.

In terms of opportunities, broadly I think the programmable nature of cryptocurrencies really excites me. The fact that you can take contractual terms from a written contract and put them in code within Ethereum Smart Contracts, I think we've barely scratched the surface of what's possible there. We now have ICOs on that basis, but there's lots, lots more to come.

ZARATE: More on the horizon I think is the conclusion here. I want to thank you all for coming and those who've watched or listened online. Join me in thanking the panelists for a wonderful discussion. And we promise you more work in this space, so stay tuned. Thank you very much.