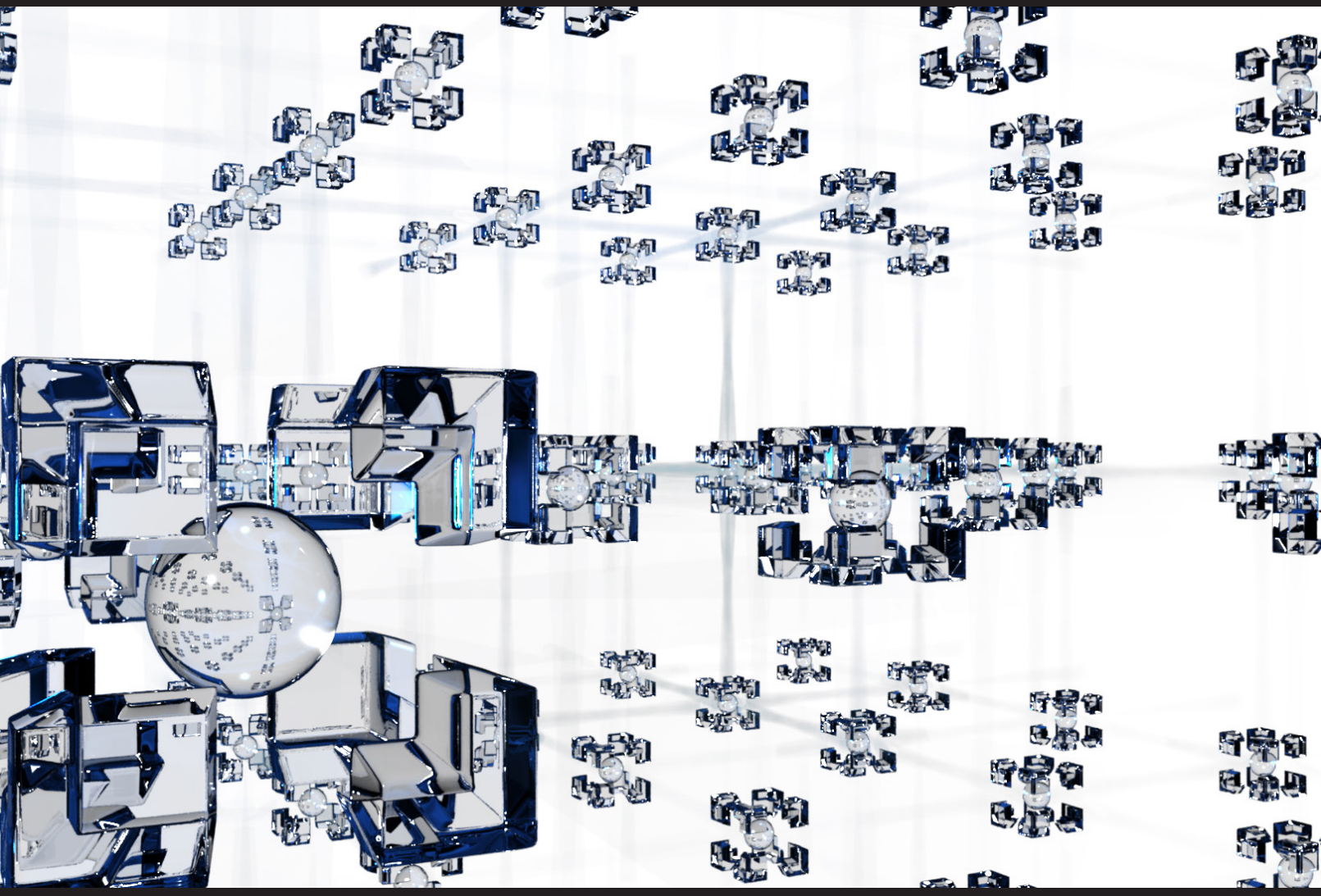
The Potomac Institute for Policy Studies
VITAL Center Presents

Application of Blockchains to DoD Microelectronics Supply Chain



Event Transcript

Cover: Alex Taliesen

2019

NOTICE: This report is a product of the Potomac Institute for Policy Studies.

The Potomac Institute for Policy Studies is an independent 501(c)(3), not-for-profit public policy research institute. The Institute identifies and aggressively shepherds discussion on key science and technology issues facing our society. From these discussions and forums, we develop meaningful science and technology policy options and ensure their implementation at the intersection of business and government.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. STUART STREET, SUITE 1200
ARLINGTON, VA 22203
703-525-0770
www.potomacinstitute.org

Contents

Image: Shutterstock.com

Executive Summary

On Thursday, December 12, 2019, Nikhil Shenoy from Colvin Run Networks presented his talk "Application of Blockchains to DoD Microelectronics Supply Chain". Nikhil reviewed some of Colvin Run's microelectronics blockchain work, including the COPIA Project for DMEA, and talked about the application of blockchain to the DoD microelectronic supply chain to address some of the current security challenges. Nikhil's talk focused on the importance of the U.S. semiconductor industry and included key points on private vs. public blockchain use cases and creating a "risk profile" record for microelectronic parts. He advocated using a "fit for purpose" approach for implementing secure ledger enabling tools. He also made the important point that Blockchain is simply a secure ledger technology; appropriate Policy must also be made for how to implement such a solution. Audience questions included identifying potential security problems, the looming policy decisions, incentives and tradeoffs of blockchain use, and approaches to blockchain use in software.

Introduction from Dr. Michael Fritze

Good morning everybody and thank you very much for coming it's great to see such a good turnout but then it's a very timely topic so I'm sure this is on a lot of people's radar screens. My name is Mike Fritze, I'm a Vice President at the Potomac Institute for Policy Studies, where you are now, and in case people don't know we're a science and technology think-tank which is independent, nonprofit, and nonpartisan - focusing on strategic science issues for government policymakers, so a lot of work for senior mucky-mucks in the government on science strategy and the impact of science on policy. One of the big things that's in my own particular area of interest is micro-electronics and supply chain - that's the speaker today who's in supply chain. This is very much in the news these days with all the Huawei concerns and supply chain security - there's a lot of language actually in that in the soon to be passed National Defense Authorization Act on microelectronics supply chain stuff so when you have a few extra minutes you can read that. There's a lot going on in the government in supply chain and electronics, which is today's theme.

I have the pleasure this morning to introduce Nikhil Shenoy. We met at the Trusted Electronics Conference at Crane, really Indianapolis would put on by Crane. Nikhil has a lot of entrepreneurial experience in a number of different areas including security software, doing software for security purposes, and is currently the CEO of Colvin Run which is a startup company doing a bunch of security software stuff but particular blockchains are of interest and he is doing some work with the DoD on applying blockchain to supply chains. This is a very timely topic which is why I'm happy that Nikhil agreed to come here today and speak on this.

Nikhil Shenoy's Presentation

Thanks Mike, good to meet everyone. Great to be here, this is an important topic. I've learned a lot about micro-electronics and blockchains since we've been working with defense and micro-electronics activity since last year.

What I want to talk a little bit about is the actual problem set. We've seen several people talk about this before. But I want to talk a little bit - kind of summarize where we're at today, talk about blockchain - why it's relevant and why it's not relevant. As an example: peanut butter is great, salmon is great, but peanut butter and salmon – it depends. Blockchain doesn't solve every problem, but I think micro-electronics is one of the few good use cases out there and we'll talk about that and the particular implementation that we use is using open standards, not just open source but open standard, so we'll talk a little bit about that and trusted assured microelectronics that is one of the initiatives in the marketplace today, particularly being led by defense because that's where the most immediate sensitivity is, but I believe is going to become boarder as microelectronics becomes even more in that market place.

If everybody here has a cell phone in their pocket, or you can talk to your car now in a lot of cases, or you have a backup camera - there's micro-electronics literally everywhere. Even my four-year-old's drum kit has the ability to record and replay the drum set she plays, but I don't know what else it is recording. The semiconductor industry as a whole is enormous, it has been close to a trillion dollars, with billions and billions of dollars – on that kind of magnitude, but the United States has been the clear leader traditional. It's the number four export for the United States after airplanes, oil, and automobiles and even in those industries microelectronics plays a key component with the rise of IOT and other technologies. At the national level, from a policy perspective, China is investing close to 200 billion dollars, north of 150 billion, a point where the numbers get very large and so quick - and nowhere is this bigger, like Mike said, with Huawei's push for 5G. With 5G we're going to have this kind of proliferation of micro-electronic components that are listening to every type of communication and we want to be very clear about where the microphones came from and where those communications are headed.

At a personal level, and this is top of mind in the media as well, so about a year ago now, and this is somewhat in question - there was a Chinese hack where they installed a dialect that went into a bunch of servers of motherboards that just listen. We don't even know what really happened or what they did, it was a lot of effort and it was more of a test than a real incursion, but it didn't happen, and it is you know something that got a lot of attention. this was actually kind of scary I saw this demoed at the same meeting Mike (Fritze) and I met at, the Micro-electronic Integrity Meeting (MIM), it's called the OMG cable. If you take this innocuous looking cable and plug it in to a computer then the attacker has full control over your system and access to your whole network.

(Michael Fritze): There's a lot of free ones at airports by the way.

The other thing is anybody who has a Nest in their in their house then also has a microphone or other wall, so this is something that I think a few people might know about. What's scary is: what else has microphones? Right now my kids drum kit has a microphone, but what else? What other cameras, sensors, and widgets are all over the place? Another example, just to make it a fun thing I guess since were eight days away from the end of Star Wars, is net breaches in trust upstream can compromise even the most operationally secure systems. It's kind of a toy example but you have malicious insertion into a large system - Galen Erso over here and then Ackbar reverse engineers is it because the plans get in the wrong

hands and you have a catastrophe.

I like to show this slide because this was the DoD slide and it's hard to read sometimes but let me talk about malicious insertion and reverse engineering and all the other kind of potential pitfalls that could be in micro-electronics. This diagram has been around for a while and it was presented at NDIA a couple years ago and in fact it was actually republished this week, there was a trust and assured micro-electronics forum in Gainesville Florida, a team form, I recommend everyone look it up and if you're interested download the paper which was just recently published. DoD is looking at this through the eyes of a holistic approach they're looking at end-to-end security and the initiative is called Micro-electronics INitiative for Security and Economic Competition (MINSEC), so that's the context of where we're at from the state level down to a personal level and the implications from the DoD. What they're trying to do is they're implementing and demonstrating assurance capability with transition partners. There are all kinds of initiatives on the street and many other organizations involved like the Air Force, DARPA, and others that are looking at how to kind of secure the micro-electronics supply chain.

With that I'll introduce Colvin Run Networks, as Mike said, we're a start-up - my co-founder and I went full time in 2018 and we have a team of advisers, engineers, and data scientists, with a retired Air Force colonel on our board as well. We are working on the blockchain with digital Bazaar, these are the guys that actually wrote some of the World Wide Web Consortium (W3C) standards, that we'll go into in today's presentation. We also working with Dr. Cameron Patterson who is an Institute of Electrical and Electronics Engineers (IEEE) member down at Virginia Tech. Colvin Run is in its first full year business in 2019 we've been fortunate to win four SBIR Awards and we're using them in the traditional sense as angel investments almost as phase one, looking at phase two as seed. The one of interest for here is called COPIA, which is Latin for supply. COPIA chain is the product that we've built that's a micro-electronic blockchain to capture a whole bunch of different types of information and then securely curate and distribute that information in a meaningful way. All the work you're about to see here was funded by the Defense Micro-Electronics Activity (DMEA).

Let's talk about blockchain just for a quick second: Bitcoin is not blockchain, the same way email is not the Internet. Bitcoin is a use case of the blockchain, currency is one example for how the blockchain can be used. Bitcoin is the first decentralized digital currency, whereas blockchain is a distributed data structure where transactions are recorded and approved peer-to-peer network. I'm going to just go into very simple terms - if you want some technical stuff there will be time in the Q&A. Let's talk about how it works: so, I want to give somebody some money. Today if I have ten dollars in my checking account but I write a six-dollar check to this gentleman here that's six-dollar check to this lady over here – it's not like two dollars show up. The first check might clear and the second one might bounce and there's a whole clearance, that's why it takes three days to make sure money doesn't appear out of thin air. The problem that blockchain solved when it came out in the 2009 Satoshi Nakamoto paper when Bitcoin first came out - it was the double spending problem. How do we make sure that that doesn't occur? The real breakthrough in cryptocurrency, the first real big use case of blockchain is in the way that that transaction occurred, and incentive structure was a real big breakthrough. So again somebody requests a transaction that they want to pay six dollars and there is ten dollars in my account, the transaction is broadcast to appear to peer network who then approves – ok Nikhil has ten dollars he's going to pay six, the network of notes validates the transaction and multitude of other transactions and puts them together in a block, and then that block is added cryptographically to the other existing blocks in the chain and then the process repeats itself and the transaction is complete. My six dollars were transferred, I have four dollars left and then that record is distributed all over the place.

Here is another illustration that I like from CD Insights that kind of talks about where this came from. You might have a physical token, so I had 10 points and I gave six to somebody or there is digital transaction where maybe you do it through a credit card so I'm pre-approved to spend ten points and I do that. What a distributed ledger does is it takes that trusted third party ledger and really introduces inefficiency, that's the big breakthrough. Now I'm incentivizing people to verify that transaction and have them participate without any third party telling them to do so. It's not like I'm paying a credit card company to verify that, when a merchant pays three percent, what I'm doing is that by verifying it myself the system pays me inherently and that's what mining is. I'm getting paid to give my resources to enable these transactions and that's the breakthrough is that you've had billions of dollars' worth of investment in blockchain infrastructure without a central authority, kind of mandating it, really leading the way. Just inherent to the system itself is the incentive structure. That's what a blockchain is about it's the distributed data structure and cryptocurrency is a public blockchain where anybody can participate. A private blockchain, I believe, is a completely separate technology for cryptocurrency but the same principle of taking information and sharing it in a meaningful way to drive common gains. When a blockchain makes sense is when you have multiple parties with different incentives, you might have regulated boundary conditions, so people know exactly what's within their scope versus not in their scope, but they interact with those other scopes in a meaningful way and they have data that's actually shareable. Just if I share data it doesn't mean it's useful, just because I have data doesn't mean it's useful. But when I have that certain kind of nugget that I can use in my operations that can influence other operations in a meaningful way that's actual shared data.

What I want to go through here is my own example of a government blockchain use case. Suppose you have a traditional information flow between a state agency and the municipality, like the county office, and then a constituent business and then you have multiple stakeholders that want to show control and retrieve data for a product. Now say I want a state-level audit and that causes a lot of work - people have to go through each of their own independent systems, compare that versus other upstream and downstream systems, it gets aggregated and broken apart and then put back together many different ways until it leads up the chain into an amalgamated form, so they get that result. Along the way you have less resolution, data losses, but you have multiple parties with the common goal of getting the information that's needed to be compliant. You have clear boundary conditions where the data exchange is happening and there's certain audit data that's been mandated right so it's very clear about how that would work. Let's take the exact same situation and install a blockchain. The way I think about this is suppose you have a water balloon and now I'm going to put some effort into the bottom of the water balloon and squeeze it, so the water is more distributed throughout. If I had a lot of work in the back end here, I'm going to put some effort to make that work happen earlier on upstream. Now people are sharing the data actively in a blockchain, so that's what that data represents, and you're adding complexity. You have a ledger that everybody can see specific information about it, you might have some data that's off chain - so the data that's mine is mine, but the data that I'm supposed to share anyway gets shared and I can add new functionality on it. That's what a smart contract is, now a smart contract for those you've heard of it, is not smart and it's not a contract, it's just a code. If blockchain is just a distributed database, a smart contract is a distributed stored procedure, for those who are familiar with legacy databases, it's just code. What's interesting here - I'm going to quote this gentleman from IBM who told me about this and his idea is that with a blockchain set up this way - it's the foundational layer that you can add new use cases on top of it, and that's the other breakthrough.

If cryptocurrency had new incentive structures - it's the new productivity and use cases that can be

built once a blockchain is enforced and in place that's the breakthrough on the private blockchain side. Now what happens is that the audit becomes much simpler, because it's front-loaded. Because the works aren't done - the audit can be continuous, you can have new types of audits where things are done continuously, you could have in process compliance so that things get addressed earlier on in the supply chain rather than having to react to things when they're broken.

If you think about one of the most famous blockchain examples is Walmart's mangoes where, for those of you that aren't familiar to give a 30 second story about it: Frank Yiannas was the Vice President of Food Safety at Walmart and he wanted to recall a pack of mangoes. It took his analysts a week to figure out three potential farmers where it might have come from. So, they thought they could do better, they started using a blockchain, this was also done with IBM, and they were actually able to, through the pilot program, tell you which row of trees it came from in three seconds. That's the real power of watching fights by kind of rearranging some of these workflows and the way information is handled and shared you can do things a lot better and faster and ultimately cheaper. Instead of how to recall all the mangoes from three farms, be able to recall certain packages and drive a real Return on Investment (ROI) when these types of things happen. This was similar to kind of drawing here, this is the link here and I'll send the slides around for those who want it, they actually put this type of architecture up on the internet. This is called TradeLens - this was again from Maersk's blockchain, which is all public domain, but it uses that similar idea of having the blockchain as kind of a foundational layer, where it's like the plumbing that has a lot of use cases built on top of it to enable these kind of new productivities.

This is just my quick drawing of the trade-off between a legacy database versus blockchain. You can do a lot without blockchain, in a traditional database, but there's certain cases where it makes sense just like you could do a construction site using only a shovel but there's a reason why they have excavators and large machinery. When the you space is big enough for big machines, blockchains make a lot more sense. Blockchain really is like an excavator - if you're building a sandcastle, like a lot of people do on the beach, if you drive an excavator up they're going to look at you like you are crazy, and yet that's what a lot of blockchain use cases are like today. People are kind of saying oh we could do that using blockchain, but you don't really need to. It's a very special purpose tool for larger scale applications and what that means is that even though you get better compliance, disintermediation, and robustness by spreading that ledger around - if one node goes down the entire system doesn't cease to exist because the data is the same that is replicated everywhere. You are giving up simplicity and performance and a sense of confidentiality and that's the hardest part of a private blockchain is the confidentiality. Everybody believes that data is the new oil, a new gold, so why would I want to share that with my nearest competitors unless there was a clear ROI? The challenge of blockchain is nailing that use case down in terms of what is the real benefit to every single stakeholder along the way. So that's what I really wanted to say about blockchains, I know that it was very handwavy, but I promise to get to more details in a minute.

(Audience member): well you talk about public and private blockchain but what about community blockchain? Does that fall into one of those classes?

Like a hybrid blockchain?

(Audience member): well we call it community but yeah.

I mean I think that that to me falls under a private blockchain because to me I think the main difference is that the private blockchain has rules for who's allowed to participate. For a public blockchain, in that

sense, means that anybody can participate - so what do you mean by community?

(Audience member): well I suppose you are right, if a group of interested companies want to participate in something, I guess that is also private.

That is an interesting point because what we found when we went into this is that we are not using a blockchain in the strictest sense. There are actually components of a blockchain that are very useful. So you have an electronic data vault, which is your off chain architecture, you have the ledger, which is the shared data that everybody can see, you also have the blockchain that tested that, so kind of trust banker if you will, and there is a lot of other little pieces like verify the credentials and other open standards that holistically when you put them all together you could end up with and blockchain but each of those components has value individually. Putting those together in a meaningful way is why we take a whole standards approach. Just like Legos and HDMI - you know they're going to fit together in a certain way. I didn't call beforehand and say what kind of HDMI is this, what kind of power source can I expect, because standards are there you have that plug-ability and interoperability. I think that's going to be essential for blockchain adoption that's a whole other presentation.

I just want to touch on here that interoperability is an essential component and like you are saying there's a whole spectrum of what blockchain can look. Bitcoin in a theorem is fully baked, you can plug the computer, in fact if you're sitting on your phone today you can join it right now to start participating and transacting on it, because it's fully baked. Underneath there's a bunch of individual components that are independently useful.

When you end up with something very complicated like the micro-electronic supply chain where there are thousands of IP cores on a single chip, with thousands of different provenances and pieces you know all around the world - you want to have something that's a little bit more fit for purpose. I'm going to talk about what fit for purpose means in a minute, but we use something called Veres Delta. Digital Bazaar, our partners, who are part of the W3C standards committees have created this platform to build fit for purpose blockchains using the independent components.

Let's talk very quickly about the best problems that blockchain addresses. I think the best one is identity, I didn't have a good War Dogs reference, so I went with Super Bad, and here is McLovin, but you want to have a way to verify a credential. The thing is here - I want to go buy a bottle of bourbon from the Virginia ABC store and I'm telling this guy how much I weigh, I'm telling him my eye color, my home address - why does that take bouncer need all that information when I just want to buy a drink and show that I'm 21? So, what that does is it actually enables you to say - well the state of Virginia attests that Nikhil is 21 and has been 21 for a very long time. So that's one thing that solves is that where identity might be overly packaged, you can decompose that in a trusted way.

The other thing that I've found it useful for is in the meaningful aggregation of information. Credit report to me is one of the best ways I can think of that blockchain will speed up the process. You can make a credit report today, and they don't use blockchain, but it took them 20 years to build it. The system about to show you at the end of this presentation - we've built it in two and a half months using blockchain people. The credit report is really, really interesting because it gives you that risk metric. Everybody in this room who's ever taken a loan or a credit card, all that activity is logged kind of passively. Every time you swipe a credit card you don't fill out ten forms and tell them this is what I'm doing, but

that's kind of the way microelectronics is done today. Before I accept the component or field a component there's a lot of paperwork and design complexity because of the compliance and contracting and all that stuff that goes into creating especially sensitive microelectronic systems.

The approach we're taking at COPIA is almost like a credit report for micro-electronics. We have very specifically metrics and standards that we're putting together, using these blockchains. We have electronic data vaults, and everybody has their own off chain data and the private data stays private, but by creating a verifiable credential for each micro-electronics component, we can create a risk profile for that chip. Has it spent a lot of time overseas? Does it have certain IP cores in it that could act as back doors? What are those standard metrics? That's where the research is right now and we're working with several partners who are talking about how the metrics come together. The credit report doesn't tell you your income for example, that's very private, but it will tell you how much debts outstanding versus what's taken versus what you're using. It'll tell you the length of your oldest account, it'll tell you a lot of information in that way, so what are those metrics that people can use to make their own risk determinations of whether to field a micro-electronic component, and that's what we are working on.

Again, this is all funded under this contract through defense micro-electronics SBIR. We actually built the system, and I'm now going to talk about bringing these two things together - microelectronics and blockchain. This is the work that we've done and are continuing to do and we're looking for additional partners for pilot programs as we speak. There are two major groups of thought in the trusted and assured microelectronics space. One is trust, which some people might call protection, and it was Dr. Lisa Porter at OSD, yes, she mentioned this in Detroit that you don't want to talk about trust, you want talk more about protection. But the idea of trusted micro-electronics is kind of an older method where I know you, you know me – handshakes, I trust your process, I know everything about you, and therefore you're allowed to be a trusted supplier of micro-electronics.

The newer way, the way that a lot of DoD is headed and thinking about is in quantifiable assurance, which is more along the lines of a credit report, but again I believe that you have to have both. In order for me to have a credit report I have to go through a trusted process, I have to apply for credit, I have to have the ability to take these micro loans every time I want a stick of gum, there's a whole trusted architecture that supports that quantifiable assurance and that's why the credit cards works. I believe we have to bring these together in a meaningful way and that is methodically aggregated, the data comes together it in a way that people can actually use, it's actively curated - so it's not just data but actionable data securely distributed because micro-electronics are so proprietary there's a lot that goes on in those data changes –

(Audience member): so those data for your quantifiable assurance – do they exist as of today?

They exist, really the question is what you want to do? There are probably thousands of attributes that you can create for each micro-electronics component. Whether you want to do the physical attributes of it, the measurements of it, or you want to think of the number of IP cores on there, the throughput of it, there are all kinds of stuff.

(Audience member): So, are you using assurance in the way that the US nuclear weapons establishment uses that term?

I don't know.

(Audience member): - in terms of basically evidence that proves that a given electronic component of the nuclear weapons will in fact perform as advertised.

Yes, so that sounds that sounds aligned, right - will perform as advertised. I'm assured that this system will act the way I wanted to, it's not going to take all my targeting and move it by 10%.

(Michael Fritze): but I think this is more of a provenance, I'm not sure this actually is a functional assurance, this is more provenance of the reference.

Well it could be, and this is where the research is happening right –

(Michael Fritze): so, there's a great question: what should be part of this?

I actually have a slide on that, so I'll show you, but the idea here is: what are those things that we need to know? What is the debt to income ratio of a micro-electronic component? Should it be test results that talk about some kind of metrics that way, is it simulation results? Because the supply chain is so complex there's actually no limit to what can be recorded but it's a question what can be actually recorded. What are people willing to say about a component without totally compromising it, does that make sense?

(Audience member): yes.

So again, that's exactly where the research is. I won't go into too much detail, but the idea here is that you can break it down into integrity and confidentiality. Integrity, that you said, is the provenance. Confidentiality is more about functionality. What brings them together is accessibility and actually having that information available.

This is the slide I was just talking about where you want to have the standards and metrics of user experience and there's all these subcomponents and this is where the active research is going on. This technology piece is the only one that we've addressed so far at Colvin Run. We've built the technology, great, you could take the technology throw it out and put Hyperledger fabric or whatever blockchain you want, or not even use blockchain and it's useless with all the rest of stuff around it.

(Audience member): Can I just ask you a question? Going back to your last slide – has anybody in DoD accepted this framework – this trusted and assured microelectronics or is this where you are working?

This is my opinion --

(Audience member): your opinion, is not a DoD stamped, accepted definition – is that right?

No, I don't know if there is one. I know that there are some in trust that's been around for the better part of two decades, assurance is up and coming. You'll probably see something similar this discussed at the upcoming breakfast in January for the NDIA's Electronics group and they have updates on this kind of thing every year. This is just what I put together because it's the way I think about it, having been in it for a year as an outsider.

(Michael Fritze): I think, Taffy, and we'll talk a little bit later after the meeting, but I think it's partly under development, because having read the NDA language - there is mandate to the Secretary from Congress that says I want a plan for a trusted supply chain. Present me a plan and something like this could be part of a plan for a trusted supply chain. I don't think there is yet a plan

(Audience member): I would agree, I can say at DARPA we have two programs where blockchain are considered. Shield is one where we have in integrated the dielet, which is a small chip, with IBM the Hyperledger and a new program called ACE where we are building hardware trust right into the chip designs and also will be linked into blockchain, potentially blockchain enabled mechanisms so you can track all new chips being manufactured.

What's interesting on both of those, DARPA SHIELD (Supply Chain Hardware Integrity of Electronics Defense) and I've talked with Northrup Grumman about some of the stuff they did and also IBM on DARPA SHIELD, and what's interesting there is that there's actually any number of entry points to a blockchain. It's not like every single thing now has to have a SHIELD dielet on it, that you have to read like this, there could be - there's another company called DUST Identity which is making the rounds at DoD. They actually sprinkle like diamond dust on electronic components and create unique hardware keys. So those can both be two different end points that wright to the same blockchain.

(Audience member): well looking at it from blockchain perspective the actual trust is in whether it's a small chip or dust, the question is if some kind of unique identities are embedded into all the chips manufactured - can we track billions of chips through the supply chain? And is this an appropriate technology?

(Audience member): the work that is going on right now at IBM and at other places as well has to do with what you're just describing - understanding the supply chain having the distributed ledgers where every activity can be verified by a whole variety of players and so you've talked about food safety, at Walmart, and Maersk uses blockchain to track all of its shipments all over the world and that's why it's very valuable for them in terms of managing their distribution and managing supply chain security of their items in a widespread distribution chain. It sounds to me, like what you're describing is really in keeping with what is happing in industry very broadly.

(Audience member): so, there's the main specifics for all of this, like for instance when we started working with IBM it became clear to us that they didn't really know anything about semiconductor manufacturing.

(Audience member): well I won't say that.

(Audience member): so, let's just say the blockchain group –

(Audience member): that's the blockchain group, it is a different group entirely.

(Audience member): so basically, we have to try to help them learn about - what are the fab floor appliances that have to exist? What does the interaction with the automatic test equipment in the semiconductor foundry have to be? What happens during packaging? What happens during manufacturing? Walmart is a good domain; micro-electronics manufacturing is another domain. When we start talking with the distributed ledger people, they did not have awareness, so we had to help them bridge that.

Let me address that – that's what I'm going to talk about, so today it's a fragmented vulnerable supply

chain, I think to your point, where everything is done on a one-off basis. Every supplier has their own security measures, Microchip Corporation which we're working they used to be Microsemi, they have their own secure programming process flow, SPPS. Xilinx has their own methodology, Intel, Samsung - everybody's got their own kind of security pieces. EDA vendors so Synopsis, Cadence, Metro Graphics - they all do a similar function, but they do it very differently. They have their own flavor of EDA electronic design assistance.

So, it still works but the way I would argue is that today we're in a Craigslist world, where I can buy sports tickets on Craigslist just like I can do it for free. I can create IP cores from different repositories but it's not the best version of itself there is still fraud, you might not know exactly what seats are getting, you might pay floor seat prices for an obstructed view without really knowing it because the experience isn't there. There's a bunch of noise here, sports tickets don't even show up on there, but with COPIA Chain, it is an openly governed architecture. This is where the fit for purpose comes in with standards, metrics, and use cases. I think a good illustration of that really is fit for purpose. For the purpose of buying sports tickets - you use something like StubHub. This really brings it to life to me as an analogy because you can see that there's a standard way of looking at every stadium, I'm able to kind of click around and there's a very common user interface, whether I'm in Los Angeles or Camden Yards – it doesn't matter. The point is that I can buy tickets in the same streamlined way. I have metrics, so whether its lowest priced, best value, best seats - I can pick my seats the way I want and there's a level of quantitative insurance in that when I buy a ticket I can actually see the seat, I can see who I'm buying from and, I get a digital version of it that I can use right at the gate. That all collectively is a user experience, knowing that there's also a policy behind it as a backstop. I don't think there's anything quite like this for micro-electronics today, in fact, one of the key parts of MINSAV, which somebody mentioned here in AFRL, is that marketplace. Whether a blockchain is part of it or not I think having that fit for purpose architecture is going to be important.

This is what we did, this is about a 20% of our reports, and each of these blocks is a data model and we actually did an analysis of different blockchain underlying tools and we've done the analysis, and this is where we kind of ended up, right now. This is not intended to be a pretty picture; it's intended to be a display of deployment. There's an actual clickable demo that takes an A380 flight controller and enables us to see different components of it, but again, the next steps are getting the standard security metrics, user experience, etc. built on top of this blockchain architecture so you can really deliver that trusted, assured microelectronics environment. That's where Colvin Run is working now, and we've been talking to IBM and several others.

This is actually an interactive demo, I wasn't brave enough to do it, but the idea here is that each of these blocks is an electronic data wall that has its own set of information that won't be shared broadly. Here we have a god view, so somebody who has been granted permission by each individual planner to see all the underlying pieces, and we've done a blacklist. Individual IP cores, so this representative here, that's the individual IP core that has been blacklisted. So, you can see the red is the entry points and the orange are the contaminated components. I call this my mangoes for micro-electronics, where we can do a very targeted recall of specific pieces.

(Audience member): so then what happens when something's blacklisted? Does a company get slapped on their fingers; do they get a 2.7 million dollar fine like Boeing did for counterfeit parts? What happens? Identifying the problem that is only in half the solution?

I agree, and that's where --

(Audience member): so, the rest of this also needs to be modeled as to how to deal with the discrepancies?

Correct. So, to your point, that's exactly right, this is just the technology. Policies have to catch up, the securities have to catch up, the repercussions from participating in such a system and incentives to do it, the standard metrics and use cases, there's a lot of work to be done, but the technology was a part that we could at least start with and then began having these conversations.

(Michael Fritze): So, for instance, I'll just - to make it concrete. If elements of this were mandated, if you could say - if you want to sell parts to the government, let's say for example, you need to join this chain. As an example, that could be policy.

That's the trusted part, so today if you want to sell components for Defense Micro-Electronics Activity (DMEA) approved systems you have to be a trusted supplier and I think that's still going to be true in the assured world but some of the complexity of the design process might be reduced, starting by technology, is the angle we're taking, but to the gentlemen's point in the back - you're right. The incentive structure is not clear. I don't know that somebody would participate in this unless there was a clear ROI, like I can sell five times as many components, it's just that now I have liabilities, but maybe my supply chain is stronger because now I'm thinking about these things and I have a way to kind of proactively say "oh this part has been blacklisted, I'm not going to put it in" --

(Michael Fritze): it has to be good for business –

(Audience member): it's not enough of a consequence then there will corruption.

Yeah, and that's true. Any system will have corruption. You're not going to stop bad players from making bad plays. What you want to do is you want to reduce that, and again security, compliance, all of that - none of it's a destination, it's always a journey. I don't know if the internet was good or bad for security, it just changed the game and there's benefits with some clear things that we're trying to address still. I think that will always be the case, but again the technology is just where we're starting. We're a 12-person company, we're not going to do the policy piece of things which is why I'm hoping to engage with people here I don't really have much left, there's only really one slide. This is a partial summary of some of the DoD initiatives that are going on - the team forum, again that's just closed this week. I encourage everyone go to https://www.tameforum.org and download the PDF there. NSWC (Naval Surface Warfare Center) Crane Division, MIM (Microelectronic Integrity Meeting) – that's where I met Mike, they have that every year. So MINSEC is the overarching initiative that I mentioned, there are two vehicles that I know of that have the funding for it. One is AFRL (Air Force Research Lab) MINSAV (Microelectronics Innovation for Next Generation System Advancement and Validation), that's on the street now, and the S2MARTS (Strategic & Spectrum Missions Advanced Resilient Trusted Systems) OTA (Other Transaction Authority) through the National Security Technology Accelerator (NSTXL), which is another piece. We're working with Defense Micro-Electronics Activity (DMEA) and JFAC (Joint Federated Assurance Center) has also been involved. There's also a component of the Army called Cornerstone is doing some trusted work on FPGA's and things like that. There is a lot of individual components going on, if anyone has an organization chart that would be great.

(Michael Fritze): this week's organization chart.

But, that's really all I had. So, thank you very much and I'd love to keep the conversation we still have 15 minutes.

(Audience member): rightly so, you skipped over a lot of the details on how blockchain works but in my understanding at least central to that is the function of mining which is the idea that the distributed ledger is in the hands of the people given math problems and they compete for the solution of the math problem - brute force, and it's essential that those people remain distributed and anonymous. At some point if this becomes pervasive you are going to run out of miners, a. and b. I don't know how you are going to incentivize them. With cryptocurrency they are incentivized by getting to keep something – how are you going to pay them?

This is where the currency is completely different than the private use case, like the community use cases.

(Audience member): so, there is no mining –

You don't need them, correct. So proof-of-work is the traditional 'I'm going to burn as much processing power I can, find the number and it matches the hash and I'm allowed to mind that transaction' There's a few other mechanisms out there called POET (Proof Of Elapsed Time), there's Proof Of State that's got it's own set of issues where you're saying that I own a certain piece of the network therefore I have say in that. Or there's the fact that you just have a voting mechanism, Hyperledger fabric uses this sense of order rating peers in order to sequentially vote on how pieces get written into the blockchain.

(Audience member): I've read reviews of many of those and the general conclusion, at least that I come up with, is they are all less secure than mining is, but they all have vulnerabilities that can be exploited, more so than mining. So, you can do miner-less distributed blockchain but you're going to have to put up with security that is not as good as blockchain as ordinarily advertised.

(Audience member): I guess you have to accept some level of trust in your private blockchain –

(Audience member): if we are back to trust, all of this goes out the window.

I wouldn't say that. I wouldn't necessarily say that, I wouldn't say it goes all out the window, because I think there has to be an element of trust in any system. If someone takes my credit card, I'm S.O.L. but that doesn't mean my credit cards are useless.

(Audience member): but the beauty of mining is the amount of trust that you have to have in the miners rather than the system or the cryptography is low. As you depart that then trust becomes more important at some point, you're now trusting in the same way that you would in the conventional sense and what changes that?

I agree, and maybe blockchain isn't the answer, but the idea of having that credit reports style infrastructure whether you use blockchain or a bunch of honeypot databases.

(Michael Fritze): if I can sort of rephrase it, because these are good questions - just think of it more, maybe it's not the blockchain per se, it's are there better ways of doing a digital ledger for supply chain, maybe that's the way to say it. You can borrow elements from blockchain, but it might not be a pure blockchain solution.

This is an exploration of how do you think more secure digital ledgers and blockchain may be part of it, it may not be part of it, there may be elements of blockchain.

One good question for suppliers would be how do I even work with this? Whether I am Global Foundries or a large provider – I have ten thousand IT systems. How am I going to have an authoritative anything of my own, versus providing information to a public forum of highly propriety data for my customers? That's one of the things that we are looking at right now – like an electronic data vault that everyone owns independently, a public ledger that you write only specific information to but what that information is – we've cast a very wide net so that's what this is intended to do, this is this to me is a very wide net and potential data sources and as we go through pilot programs we will learn what people are, and are not willing to provide. If I told you that now every time you want to use your credit card you have to provide your W-2 from the last three years - people might not use credit cards as much anymore if that is the case.

I'm trying to use toy examples, because I don't really know you know which of these data sets people are willing to share.

(Audience member): so what would be the strategy if you have a lot of companies that wanted to create a community mechanism like this? And in the absence of miners, how would you set up the authentication mechanism of blockchain parts.

So, in the pilot program that we are proposing right now, and is in prototype development, everybody has their own electronic data vault, we figure out what they are willing to write on there, and then we only write the hash of that data to the blockchain so that way you can verify certain pieces. We do this because the part that comes from the photomask is going to be very different than the data than the packaging guy puts on there.

(Audience member): so, would that apply to a pre-competitive fab space like inet in Leuven, Belgium where basically a bunch of companies have come together to prototype micro-electronics pre-competitively in the same venue and having it should essentially trust the fab equipment that's there?

Yeah, I mean you have to trust your own equipment –

(Audience member): no, but this is a this is a pre-competitive shared environment.

So, where people have certain tracks on the wafer or something?

(Audience member): they have access to fab equipment, that's very expensive

Yeah that could be interesting. Yeah, the tape outs are very expensive. I think, and this was your presentation, that I think it was 5-20 million dollars to just do a single design run.

(Audience member): this was just to do the tape out.

That's why a lot of what we're doing is working with people, and even before that at the simulation stage on what data can we collect.

(Michael Fritze): quick follow-up to what Lee was saying - so the stuff, and I know it's an early stage of deployment, but the commercial implementations are with the ones that are at a serious prototype stage. What percentage of those are public versus private? Do you have like a read – is it more common to do a private blockchain solution? A public blockchain? – because there's a lot of overhead in public.

Yeah, it's more common to do the private – Taffy if you want to talk about IBM, they've done hundreds of them, we've done three.

(Taffy): I have nothing to add.

I think in general, I believe, Hyperledger fabric is private implementation, that's what people are doing here. It's kind of weird, it's like the Internet in the 90's with the Cisco internet, you have the MCI internet and they are all slightly different, people had different ideas on how to own the internet

(Michael Fritze): I think you started correctly but there's almost a one-to-one mapping, which isn't always correct between Bitcoin implementation of blockchain and the concept of blockchain. It's a spectrum of technologies.

Blockchain itself, like I said, is about ten years old now and in 2009 all those components were also technical, so it's not like anything in blockchain is particularly new. Bob Kahn did a document object repository patent in 1997, that basically had the same idea, but it just didn't catch on as well because there wasn't money to be made. Even Bitcoin, when it became popular when the price went through the roof for reasons I can't understand.

(Michael Fritze): I don't think anyone does.

Once you found that there are college bros are becoming multimillionaires, I think that's when blockchains became a thing. Now it's just an interesting term to use because I think more people want to learn more about it, like the Gartner's trough, but I spared everybody from that in this presentation but you know I think we're heading into that trough which is a good time to really learn, let the tide go out. I believe that this is one of the use cases that may be useful whether we use a blockchain or not. I also firmly believe that public blockchain like cryptocurrency, and a lot of people call it a distributed ledger technology give some other name to private blockchain because you don't really need a consensus algorithm if you have that community all set up.

(Audience member): can you talk about the community being all set up – can you talk about the some of the risks, if I understood correctly you are talking about the problem set being fragmented and vulnerable, the risks of not having standards or what are the incentives to standards?

I mean standards are double it sword because now everybody knows what you're doing, so if I want to attack electric grid I kind of know how it works. At the same time, that's that small piece of danger versus the general benefit of having a standard and there's a lot of debate about this by the way - open source versus open standards, which one's actually safer. But having an open standard means know its open- everybody knows exactly how to game the system; I think to someone else's point. There is risk, but I think the benefit is and then incentive is the ability to expand supply risks to field more modern micro-electronics more quickly.

There was a chart at the MIM it said commercial innovation goes like this and then DoD was kind of leading micro-electronics and now it's less than 1% of the market and now they're down here at the 60 nanometers (nm) where the market is going to 12 and 7 nm. In order to catch these lines, back up in and get DoD innovation back on the commercial curve is what they're trying to do with quantifiable assurance and standards and things like that, am I right? --

(Michael Fritze): no, I mean that's a great way to say it is look at what are the companies at the leading edge, right - there's three and two of them are overseas and the one that isn't just makes processors pretty much

(Audience member): how do you get to the stuff, to fidelity of subcontractors? How would blockchain solve the problem of subcontracting when you are trying to update to get the most up to date semiconductor, but that company might have to subcontract out? How do you validate --?

So blockchain won't necessary solve the problem from the technology perspective, again it's a small piece of this puzzle –

(Michael Fritze): it's a ledger right it's a written record

How does QuickBooks solve financial problems? It doesn't.

(Michael Fritze): you can put a bad number into QuickBooks.

So blockchain is monitoring – it can give me the ability to see that – oh, this guy's using pre-blacklisted components in his deliveries, so we want to have a conversation about that.

To another gentleman's point - that'll disincentivize people from putting those pieces in, in the first place. I think that's how the technology does it. I think that the standards could address that through here's a black book - we're going to publish the known bad components that you shouldn't be using. If there is a way to access that and share that information, I think that will go part of the way to doing it and there are a lot of pieces here that will be improved.

(Audience member): have you thought about, beyond the scope of this, have you thought about how you apply this same approach of blockchain to software?

I've thought about it, but its very broad, software is a lot trickier, more hazardous and more fungible. My version of Microsoft Word when I was an investment banker was different than anybody else's because I build my own macros and stuff into it, there's all kinds of things - there's no telling what could be done to software. Hardware at least is a little bit more --

(Audience member): I want to return to your StubHub analogy, that is a verified reselling, and it seems to me it is, as you say a blockchain ledger, it's not going to solve some of these other policy technological problems but it seems to be drawing entirely from provenance, trusted supplier. If you have electronics that you're looking for that are resold, are used, are obsolete, are no longer manufactured with a company that manufactured them and that company was bought - where do you see blockchain entering, or your starting point would be anything that you can trace from its original production, starting from that even today, but months or years from now in such a thing would be implemented?

So, imagine a credit report that tells you - this is their usage to availability ratio. I don't know when their first credit card was opened, but I have partial information. At least you have some information you can go on and if those risk factors meet what you need - you could weigh using that component versus security gaps or you can address those security gaps. But once you have the information there's a lot more you can do with it. Today I don't believe that's the case - where the information is even there. That's one thing, without blockchain, having credit report for micro-electronic components would go a long way, at least beginning to understand the risks of using it - does that make sense?

(Audience member): yes, I'm just wondering how much of an advantage that is over a system like counterfeit reports?

I wouldn't say it's any different, it's just that, instead of having to go to a file folder you're able to have it all on the system to be able to log that information somewhere that it can be used. If I go through several programs and then ten years from now somebody opens up a box that's been sitting there, and now I want to use this component – I don't know if it is going to solve that problem if it wasn't part of this system to begin with.

(Audience member): precisely.

I think this would be better on a going forward basis to catch up those innovation pathways. For the past problem - it's a problem that can be could be addressed by the system, but it will still take an initiative to kind of get those modern pieces up there, or catalog pieces. In fact, the DLA (Defense Logistics Agency) did an SBIR round about a year ago when he just listed a bunch of individual components for people to reverse engineer. An initiative like that would be a great way, where you reverse engineering all these individual components and test what the designs look like on a blockchain, so I know what performance to expect out of these when, in fact, something does get fielded. There are all kinds of things you could do, once that infrastructure is in place you can build new use cases on it and that is a very exciting one.

(Audience member): because of the computational expense of a distributed ledger and your scope, which is all of microelectronics, how scalable is this?

It's very scale. The point is, that because we're doing it the way we're doing it, where you have an individual electronic data vaults, and the public blockchain is separate – I didn't put that slide in here, and now I'm taking myself, but I follow up with the links if you email me, because it's all online – about how the individual components are separate from that blockchain.

(Audience member): but isn't it computationally expensive, if you are doing consensus where's the computation?

It's mostly just storage –

(Audience member): so, there is no computation –

- because what you're doing, you're just doing the hash of the information so I kind of skipped over –

(Audience member): are you computing the hash though?

You can, yeah, but not the entire network every single time. It's just the electronic data vault is saying "alright here's the data, here's the hash information and I'm going to store that." Now I'm going to say alright Nikhil Shenoy from the state of Virginia at this address, and is this old, and this is his birthday - make a hash of that information and just query the blockchain for that hash, and if it says yes I'm good to go, I'm verified.

(Audience member): We talk trust and security, but can you talk about cyber? What are you actually doing in the area of preventing and offering some resiliency or system, because it will be a target?

I think endpoint security is probably number one, garbage in - garbage out, making sure that those procedures are followed. That's where we're looking at the trusted aspect of things is following the DMEA standard, because they're the ones who sponsored the work, so we're using their protocol as a starting point for the trusted access to the blockchain itself. Once that security becomes clear and then the right experts are brought in then we'll go from there, but we're starting small. That's why, this is all prototype stuff, but you are right that is a major concern.

(Audience member): so, you use the database hacking example in the introduction, can you tell how this blockchain system can prevent or detect that kind of situation?

One example will be when I received a board - suppose I'm able to run some kind of a test on it that says: when I run everything this is the side channel analysis that looks like this, this is the side channel that I traced on here, and there was a test that went on earlier and that was a side channel that they had. I can query and say, "is this is side channel what I would expect from this component?", give some metadata about the component, and then the hash of that information should be the same that was on the blockchain. If the dielet changes that side channel at all then the hash will fail.

(Audience member): that kind of analysis – everyone who makes a product does that kind of simulation. Today the reason that we cannot detect that kind of problem is because the expected profile or simulation data is not available to me to cross check that.

This is where the research is. What is tenable in terms of the metrics? Maybe I could weight, and I the component I know that the weight is slightly different.

(Audience member): well you can also have a component, or a board, or subsystem that has perfectly expectable performance with all functions being president and correct, but functions added that you don't know about.

(Audience member): DARPA has a program under development for this exact thing and it looks at all of the attack vectors that are known and will propose a variety of defense strategies -

(Audience member): DARPA has been in that business for twelve --

(Audience member): I'm just saying specifically in response to the Jason Robertson's article, we have an activity in this area.

(Audience member): when you bring this data into this network, how can you trust it? Let's say the simulation data, or spec data for certain IP – is there someone who is monitoring or certifying the trustworthiness

of that data, or do you just bring it in?

I don't know --

(Michael Fritze): there has to be a protocol for who is allowed to join, which we talked about a few minutes ago.

That's the trusted supplier piece of it, who is allowed to write to the blockchains right now --

(Michael Fritze): you're going back to saying your current assumption is you're using whatever the DMEA requirements are to be a trusted supplier. That's their default and that's what you need to pass in order to be a contributor, but somehow there needs to be a protocol in order to join.

Correct and that hasn't been defined, other than the DMEA protocol –

(Audience member): blockchain is just a tool, it's an element in the solution but the system needs to be developed and that system is usually domain specific and has to be aware of semantics.

I'm just really glad this is going to be a report because that's going to be part of the research that we have to do and so that's great, absolutely. I think that there's a lot of value to be had in exploring things just like that.

(Michael Fritze): I like to think of the simplest thing to do this with would be an Excel spreadsheet that you encrypt. That's the simple story, and then there's a whole spectrum of more secure, more complex ways of doing digital storage, but the simplest thing is everyone puts data into an Excel spreadsheet, and you encrypt.

(Audience member): Nikhil is your company more of a services company or more of a technology company? It seems like you're providing a lot of services up front.

Yeah, we're bootstrapping, our goal is to become a company with a licensed product. Hopefully someday if everybody pays us a tenth of a penny for every micro-electronic component that ships and is COPIA approved – that would be a wonderful outcome. But we're bootstrapping, like I said we're using the SBIR program as an angel investment in phase one and seed stage in phase two. We are a bunch of data scientists doing data science, so we are consulting our way out, rather than raising money or anything like that at this point.

(Audience member): how do you compare yourself to something like Guardtime Federal or other companies like that?

There's a lot of great companies there. I'm very fortunate, I used to run a chapter of Government Blockchain Association (GBA) so I got to meet them and actually IBM spoke, but there's a lot of competition in this blockchain world. When we grow up maybe we could be as successful as Guardtime, they're a pure blockchain company so they have been enabling technology that can be used in a lot of use cases and we're trying to find a use case and really just own that one use case --

(Audience member): micro-electronics use case.

In this case, yes. We have lines of business -- this ISR (Intelligence, Surveillance, and Reconnaissance) analytics, so we're doing some work on the P-8 Poseidon program and the other two: we just got one before Thanksgiving at the F-35 pitch day. Right now, we're using a "powered by" strategy - powered by Veres Delta, IBM Watson, Databricks, and MicroStrategy. Those are our major technology providers and, in each case, we're looking at a use case and trying to hone it, learn it, and create a repeatable business that way as a way to bootstrap so we can come up a reliable product.

(Audience member): one of the challenges of these Air Force SBIRs is that they award a small amount of money for a study and then it's on you to go find a government end-user in the Air Force. Do you have those guys lined up for all of those projects that you want?

So, for SHOPMAN, definitely, SIFTR is the F-35 joint –

(Audience member): What are you working on with SHOPMAN?

For SHOPMAN we're talking to, well MicroStrategy is our main partner, I probably shouldn't mention our customers at this point. We actually have some memorandums of understanding and we're still looking for more -- so if anybody here is willing to talk about predictive maintenance and inventory management, I know it's completely off topic, but please find me.

(Michael Fritze): There are a lot of interests here, so I appreciate everyone taking the time out, and I thank Nikhil again - thank you very much.