TECHONOMYNYC

Blockchain and the Digitization of Identity

Speakers:

Daniel Buchner, Head of Decentralized Identity, Microsoft

Vinny Lingham, Cofounder and CEO, Civic

Melanie Shapiro, CEO and cofounder, Tokenize

David Treat, Managing Director, Accenture

Moderator:

Meltem Demirors, Director, Development, Digital Currency Group

(Transcription by RA Fisher Ink)

Meltem Demirors: I'm very excited to be having this discussion around digital identity and what a future around digital identity on a blockchain may look like. How many people here in the room have heard of blockchain? Just a show of hands. All right, this is great. I feel like it's impossible to go anywhere today without talking about or hearing about blockchain. So hopefully today's discussion will help elucidate some of the great work that's happening across organizations of all stripes that are really starting to bring some of this innovation around identity to the forefront of actual products, actual services that people consume.

I'm Melton Demirors, I'm with a company called Digital Currency Group. We're a little bit of a unique company. We build, buy, and support bitcoin and blockchain technology companies, by leveraging our insights, our network, and our access to capital. What that means is, we act as a venture capital firm. We've invested in over 100 companies now, across 27 different countries, which all leverage blockchain technology, digital currencies, or distributed computing in some capacity. Some are b2b, some are c2c, some are b2c, so a lot of different ideas encapsulated in that portfolio. We also build and operate companies. We have a media company, CoinDesk, which I hope you will all go and read. They are a fantastic source of news for what's happening in this industry.

We also have an asset management business called Grayscale, which has two products in the market that enable retail investors to access digital currencies in their portfolios. We also have a trading business that's a fully licensed broker/dealer for institutions who want to interact with digital assets. It's a very new company, but it gives me a lot of perspective, a lot of insight into what's happening in this blockchain space. It also enables me to work with a lot of great corporations, like Microsoft, like Deloitte, Accenture, other institutions that are all looking at helping their clients use this technology. With that said, let's just decide what is digital identity? The word identity has a lot of different meanings, so I went online and I looked it up. The internet tells me that, "A digital identity is information on an entity," so a set of attributes that are used by systems that are used to represent an external agent. That agent could be a person, an organization, application, or a device. Today we have representatives from a variety of different companies. I'm going to let them each introduce themselves, but also I want to ask them each to talk about how they conceive identity and the digitization of identity, just in a short, two-minute statement. We'll start with Melanie.

Melanie Shapiro: I'm the CEO of Tokenize. We build a consumer device that allows people to merge their physical personhood with their digital identity. We're actually launching next month, in June. The way that I think of identity and digital identity is that it's very separate in the physical world versus the virtual world. In your physical world, you have personhood. You are identified in a free country with democracy and free markets as a person and people respect you as a human being. Now, that got very complex as we had the internet and now all of a sudden, we have a digital life. In that digital life, we also have different digital versions of ourselves or digital identities.

The way I think about digital identity is it's just a set of attributes that could be pointed back to a person. The problem in this space, very much so, has been that those attributes or those digital identities that make up who you are very much are becoming disconnected to personhood. That becomes very scary, because you as a person need to have control over your social or whatever kind of identity you have in the digital world. We're building a solution to make it possible to merge your physical self with your digital self, so that you have complete user control of your identification, of your data. Without user control, the future of identity is very scary.

Daniel Buchner: I head the decentralized identity product and engineering work for Microsoft. We're using a lot of the technology that Meltem alluded to, to develop systems that can restore identity in a self-starting way to the users or any other item that they're used to identify. What I think of identity as is really self-attested and externally tested attributes. The state may attest that you're at a certain height and weight on your driver's license, for instance. That's externally attested. Your height and weight may fluctuate, and you know what it is, or you have things that you self-attest. Self-attest means, "My favorite color is green," right? I'm the authority on my favorite color, no one else is. I think identity is sort of the composition of those two things. A lot of stuff is self-attested, a ton of it comes from external sources. People's view of your identity changes, from person to person. People see things very differently and identity is actually like a prism in that way.

Vinny Lingham: I'm co-founder and CEO of Civic. I'll give you the long story. We started the company trying to solve the problem of voting. How do you allow population groups large and small to participate in democracy at scale? One of the key problems that you have to solve with that and enabling people to be able to vote on mobile phones, in the comfort of their home, security-wise, etcetera, is solving the problem of digital identity. How do you know it's that person on that device? That's the genesis for the thinking around the company. We wanted to build it in such a way that it could be globally distributed. We looked at technologies like blockchain, and we realized that we could build a global system where 7 billion people could be connected to the same system and be able to vote for their local and national governments. The biggest issue with building a system like this is that if we stored all your personal information in a central server, it would be the worst idea ever, in the history of mankind.

[LAUGHTER]

Lingham: We built a platform that actually distributed the ID credentials to devices. Your personal device holds your information and no one else's. In doing that, the risk of an attack, a breach is minimal. They have to actually steal your device. We did some trials with Intel, so we're able to store personal information on the chips. It's called Software Guard Extensions. On the actual chip you can lock it down, kind of the way touch ID works with Apple. We basically are building this massive global distributed device-based identity platform, where you can use it to login to your bank account without passwords. You can log into anything by using some sort of biometric on the device and the credentials that are stored there. Our vision is to replace passports, driver's licenses, you name it, with effectively whatever device you can secure and use.

David Treat: I lead our blockchain business for financial services and I'm the deputy head of it firm-wide, which has now given me great opportunity as a capital markets guy to get into all other sorts of other industries, which is a lot of fun. For us, there's one way of thinking about all of the work that we do supporting our clients. There's a common thread around a lot of it, which is the problems associated with today's fragmented nature of identity. Whether it's AMLKYC issues in financial services, our focus around—We've actually built and implemented a significant portion of the world's border control systems and the like. We've now formed a dedicated blockchain identity team, to think across industry in each of these modes, in each of the unique business challenges in every ecosystem and industry, applying a lot of these concepts. So taking the notion of work we're doing in biometrics to be able to affirmatively associate a human with an identity, very similar to things you're working on Vinny. That's who we are. As the world's largest independent technology services company, we get involved in every form and flavor of this.

Demirors: Thank you, that's a great summary. My goal today—we have about 45 minutes—I wanted to bring together thought leaders who represent a lot of different parts of identity systems that are being built today in various capacities. We're going to have a meandering conversation. I'd love for it to be a dialogue and give you an opportunity to ask questions as well. The point I think that all of our speakers so far have highlighted is there are many different forms of identity. As Melanie said, we have our physical identity, we also have physical cards that represent our identity like a driver's license or a birth certificate. We have digital identities, which are stored on our phones, which may be stored in centralized servers and managed by service providers. Then, we have virtual identities as things become increasingly virtualized.

You may be a different person on Twitter than you are on Reddit. People also now have increasingly virtual lives they manage along with their physical and digital lives. I really wanted to talk about the way that we can leverage blockchain technology and this idea of distributed computing, of distributed systems, of non-centralized systems, to bring new forms of security to identity, but also to start linking some of these different identities that may exist in different places.

What we mean when we talk about identity, as we've highlighted, is they're people. I think people also tie back to organizations and institutions, which themselves have an identity. I am Meltem Demirors; I am an employee of Digital Currency Group. I'm a graduate of MIT, an institution. And then, there are also different machines or devices. I have an iPhone; I have a laptop; those are all associated to me. Maybe I own a vehicle. I have a credit card that gives me the right to access certain assets, which I also own. How do I identify all of that stuff? Today, the way I identify it is I have a phone. I have a credit card. I have probably hundreds of online accounts, which are mismanaged in various ways. I'm trying to use a password manager more; it is very difficult. I think the point is, we use identities for a lot of different purposes.

Primarily, we use them to identify ourselves. How do I positively identify myself? How do I authenticate, or prove who I am? If I get pulled over, I typically hand the police my driver's license, that proves I am who I say I am. How do we actually use our identity to authorize something, whether it's a transaction or changing an attribute about ourselves? Let's start with people, we're all people, and we care a lot about our identities. You talk about identity all day, every day with your clients, with your partners, the customers you're designing your products for. In the developed world, the world we all live in, how do you think the status quo around identity is being changed by blockchain and the idea of distributed identity systems? How is your company specifically trying to address that opportunity?

Shapiro: That was a very good question. All right, our belief is very much that the blockchain enables user control. One of the most important things that we're trying to accomplish is that which is basically informed by our belief in the future, our identity, ourselves in the digital world, is represented by a private key. Basically, the future of identity is cryptography utilized distributed systems, like the blockchain. What we believe is that using a piece of distributed hardware, not an iPhone, not any other general computing device that you really will not ever have true control of your private key, we use distributed hardware. We've built a consumer product that's another piece of hardware, that I can't mention right now. You'll use that to represent yourself into digital systems.

For example, we've just partnered with a very large nation state. Later this year, we're rolling out a Tokenized version of your passport and your driver's license, to be used to identify yourself at a bar, at an airport, at a train station. Anywhere else where you have to represent your physical personhood to a digital system. That is the solution that we've built with this government. It's incredibly powerful, because you have control. There's someone attesting to the fact that I am Melanie Shapiro, I am X years old, and I have certain authorizations, but ultimately, I control the key that is my digital self. That's incredibly important. The other part of that, that I'll end with, is all of the things that make up who I am, they don't need to be aware of each other, either. There's this technology that's part of the bitcoin-blockchain, it's called hierarchical deterministic wall, our first product utilized. Basically, you have a seed, which is yourself, your person. You can generate identities or versions of yourselves from that seed, but they within some network don't need to know about each other. That's really important because I don't need Facebook to know that I have three Facebook accounts and three Google accounts and whatever else.

Demirors: Great. Daniel, I know at Microsoft you spend a lot of time thinking about identity, because Microsoft has a lot of products that millions upon millions of people use today to manage identities. How do you think of the challenge of identity in the world that we all live in? What are you doing at Microsoft in your organization to re-conceptualize that using some of these concepts that come from blockchain technology and distributed systems?

Buchner: My personal and product philosophy when it comes to the blockchain and identity convergence is that the blockchain is fantastic for a few things and it's really awful at a lot of things. One of the things it's really good at is rooting trust anchors. Things like, Turing-style proofs where you stamp the time and state of an occurrence, for instance, on a chain. That yields some value. Another thing in the identity sphere you can do with an anchor is anchor an identifier to a chain. Just think of it as a new re-imagination of DNS, but decentralized, where I can get a list of all the identifiers in the world, and find locations off-chain where their data may reside. That's identity data. It doesn't mean you don't have access to other identity data, it means that for the first time really, in the world, we have a system by which we can root anchored identifiers, and use that as the look-up, essentially for people's identity data. We're engaged in building out with a collaborative set of individuals and partners an open-source, cross-chain, system-agnostic, decentralized identity layer, based on blockchain that runs across all the common chains you would think of.

We want to do that for a few reasons. One big one, a mandate from pretty high up, is that we'd like to be in a future where you have a "bring your own identity" paradigm, where AD and some of the products we have, we're not scared of this new paradigm, they still require you to manage roles and responsibilities and all that good stuff. If you can just imagine where we're at today is sort of where you were at when you had cellphones, when they first come out. You had a cellphone for work and you had a cellphone for your personal life. Now, it just seems crazy, right? You just get a policy on your phone and that's great. I'd like to see a future, and we're building towards a future, where you have your identity, it's sovereign to you. When you get hired, say at Microsoft, they might sign you some attestations, externally attested proofs, that you're an employee, that you can access certain buildings, all this good stuff. AD would manage that, just as it does federated identity and centralized identities today. It would just be educated about this new class of identity. That's one way we're trying to use it.

Lingham: We could speak for hours on this topic, but I'll leave you guys with two parts that are very interesting. The one is, when you're using protocols like OAuth, OAuth is Facebook

Connect. When you go to a website and you click on Facebook connect, they go and check with Facebook to make sure that you logged into Facebook. Facebook tracks that data, then you're able to login to the site, and you'll be able to reuse those credentials when you go back. When you're switching between apps, you'll never have to create an account with that site, because you're using your Facebook-attested credentials to login. The problem with that model is one of privacy. Obviously, Facebook now knows all the different sites that you're on and to some extent they can start building patterns around you. Facebook is just one example of OAuth being used.

Where the blockchain comes in is if you could replace a live instance, for example Facebook, with something which is static, a blockchain ledger, the blockchain doesn't track when you use it. If the site was able to just look up the keys that you're presenting when you want to log in, confirm that you are the owner of those keys, they can let you log in. There's no trail, there's not history that the site read the blockchain for that information, and therefore you go from a three-party system, where three parties are effectively involved, to two parties, plus a static ledger. In theory, by the way, that ledger could be off-line. It could be printed on a piece of paper and they could verify keys that way. It's very private and secure. That's one way I think blockchains are disrupting the notion of trusted third parties in the world and really making it more peer-to-peer.

The second instance is one of censorship. When you look at some governments of the world, which are obviously very oppressive, and some privacy laws are there for a reason, right? Some governments have laws which don't allow you to transmit data outside the country, around personal information. To some extent, it also applies to what we do in our process, which is, we have one-way hashes, and others taking your personal information. We create a hash out of it, which can't be decrypted, so you can never reverse-engineer that. It's exceptionally difficult to do. It's probably impossible right now, until quantum computing comes in.

In the current paradigm, that one-way hash still effectively represents a token form of your identity. If that information cannot leave the country, you can't make a universal ID system. How else would you do it? But when using a blockchain, essentially the data sets on a blockchain in that country and because of the way blockchains work, the nodes would propagate the data across the world. This is why a bitcoin is particularly interesting for us, because there are 4,000 or 5,000 nodes worldwide that would have an exact copy of that record and they're not really breaking the laws in doing it. This is how the system works. You can effectively build a distributed identity system, without breaking any laws, and without transporting data out of the country. That's basically what we've leveraged to build our tech.

Treat: All right, let me try out something new.

[LAUGHTER]

Demirors: We're going to switch it up.

Treat: It's fantastic, right? Melanie, the physical association between the human and the identity, between what you guys have now talked about in terms of the system that would make that work, to be able to really change the power of flipping the dynamic, right? Meltem, from where you started, of identity right now as fragmented and is owned by the authorities with whom we interact. They're owning it for, presumably, for the purposes of the services that we're getting from them, but as we all know, there's a whole degree of discomfort with other ways it's being used.

One of the things in our client conversations that's really starting to heat up is that everyone kind of gave up on privacy. Privacy is gone. If you haven't heard any of those speeches, there's a bunch of people out there who talk very eloquently about how privacy is gone. If you're going to debate whether or not we have privacy anymore, you're five years too late. That was a while ago. I see real hope now, actually, to reintroduce the notion of actually, through the combination of these technologies and others, that we'll actually be able to reintroduce the notion of privacy. What does that mean for business in particular, in terms of our use of AI and big data, and the insights and analytics we're trying to derive from the notion of the authorities owning the identity and the data associated with it? On the positive side, if you could now, as you guys are describing, have a single identity traverse that entire ecosystem of businesses and services that you get and work with, that's great. You get much better service, let's say, from an AI implementation that's not constrained to the company that's implementing it, but can now suddenly draw from data upon your entire life, from a human perspective. That's the great side of it. The other side of it, the downside of it for businesses, if the privacy pendulum swings the other way because of what we can do now with blockchain technology and the associated pieces, they then suddenly may be locked out of things that individuals don't want them to see. That balance, I think, is going to be a really interesting conversation in the next few years, in particular.

Demirors: Absolutely. I think what all of these dialogues have highlighted is the need for trust. The issue of privacy is really an issue of trust. For me, what I think about, I was saying to David earlier when we were in the green room, I didn't really think about the way in which I divulged components of my identity before I started working first in bitcoin, which has not really become blockchain. I used to just put my credit card number, my birthdate, my address, my cell phone number, into apps, and not even think twice about it. "Hey, this is what I want. This is the barrier for me to get it. Here you go. Have it. Go at it." That's really scary, because what I'm relying on is trusting that application, that third party, to store my data, to manage it, to append and change it, but also to secure it.

We also rely on governments, as you've highlighted, to issue us an identity. If I live in a state where there isn't a strong government, where there aren't strong institutions, what does that mean for my ability to have a recognized identity, which then impacts my ability to open accounts, to have access to financial services, to have access to human rights services. Our employers have a lot of power over our identity, our banks control parts of our identity, they determine what we can and can't do with our money when we try to make transactions.

Telephone companies, hardware companies like Apple, software companies like Microsoft, and all of the different services we rely on in our modern life.

I think this takes the conversation to organizations. Organizations who issue the identity are often responsible for managing it. What we've seen with the centralization of data, is we've created basically the biggest honeypots ever for hackers to go after. If you tell a hacker, "If you hack this database, you get the identity of ten million customers and all their financial information." That's an extremely attractive target. I'll just quickly highlight a few really big identity breaches that have happened over the last year and then we can dig in to why they've happened and how we can work with organizations to try to prevent these. In the department of justice, one of the most revered institutions in our country, was hacked. The identity information of Homeland Security employees and FBI employees was taken. That included their names, their email addresses, and their phone numbers. Think about that for a moment, very scary. The IRS was hacked. Over 700,000 taxpayer records were stolen. Imagine that you file your taxes every year with the IRS and someone now has all of that data about you, which includes by the way, your social security number. That's terrifying.

On the healthcare side, a cancer care company in Florida was hacked and over two million patient records were stolen. That included information about their medical history, it included information about their insurance, it included information about their payment history. You think about the things that are most private, too. These all make me cringe, but we never really think about it in this context. Lastly, I think the biggest winner of all is Yahoo. Over one billion customer records were hacked. That number, one billion, is staggering. That is 15% of the world's population, who had their data stolen due to trusting a company that then failed to appropriately manage their personal data. As I think about that, it gives me this very scary feeling, this dystopian future where I have no control over my identity.

Let's just quickly do an audience poll. Who here has had their identity breached or stolen in some way? If you're a Yahoo customer in any point of your life, highly possible. That's a lot of people. Three people on this stage here, who work in identity and security, have had their data stolen. Dan, since you work at Microsoft, you're thinking all the time about how Microsoft is a custodian of people's identity data. As you think about the way you are responsible for securing data, what are some things you're speaking to your product teams about, in making data around identity more secure, more trusted? What are the things you're doing today and what are the things you may do in the future?

Buchner: The model that we're using to architect the open source underpinnings to the system is essentially, "Trust no one." It is okay that providers, in our instance we call these things hubs, that may live on a ton of different providers, Microsoft, Google, I want our competitors to run them, there's not competitiveness there. These stores of data though, are uniquely different, in the sense that everything that's written to them is encrypted, at the edge. We have absolutely zero knowledge of the data itself. We can only see what we're given, we're an agent, like everyone else. If you imagine Cortana in the future might ask for some permissions to your identity, it becomes an agent that can only see and base it's AI work, as you were saying, on what you allow it.

We may end up being custodians of your data and able to serve it, but we actually can't see it, and that's one big piece of this system that I think, that alone would force the threat vector down to the device level, which is still breachable any time you hit the view layer, you have something breachable. It's just much more difficult, especially with things like what Mel is doing here with the token, that adds another layer of security, where it's not just that device, it may be a secondary factor that they would have to breach, which makes it all the more difficult. Those are all things we're taking into account in our product vision, things we're building into the system.

Demirors: So David, you're advising many of the world's largest financial institutions, right? This must be on the top of their minds. No one wants to be Yahoo. I think that is clear. How do you frame, when you go and speak to a client, who may have never heard of blockchain technology, right? Maybe they've read about it. They're like, "It's this crazy weird thing people on the internet are doing." How do you explain it to them in the context of security, and particularly securing all the data and the records that they're responsible [as custodians]? How do you introduce them to that concept? How do you have that dialog and set that context?

Treat: Dan's examples highlight it, right? It's wrapping the notion around in a traditional database system, by and large, and there'll be a few people in the room who'll throw something at me afterwards, but by and large, there's a layer of security that wraps around a traditional database. When you breach that layer of security, the question is, "How much data did they get?" They have access either to entire tables or entire databases. The notion of the fundamental component of blockchain technology is a much more granular level data access, where individual data elements are encrypted by who put it there, who's allowed to read it, who's allowed to change the state of it, etcetera. That granular level data control is a huge leap forward from this notion of a layer of security that wraps around a data store. It's now embedded within the data store. That's a great leap forward. I think that's the simplest place to go. There's a stupid analogy around the excel table of: You're encrypting it at the cell level, not the excel file level, but I'll spare you that one.

Demirors: I'm going to go back to you again. I think one of the key challenges with all of this is financial services in particular, but a lot of industries that deal with sensitive data are highly regulated. I think regulators obviously do their best to stay on top of all of these new innovations and really understand how paradigm changes are introducing a need for regulatory changes. Do you think the current regulatory structure we have may limit the ability for large institutions to implement blockchain? Do you see there being more public-private partnership where those conversations are accelerating? How do you see that interaction working? The two seem a bit at odds at times.

Buchner: I don't see the two at odds, actually. When you look at the level of investment of focus that the largest financial institutions are applying to blockchain, they have blockchain labs and teams that are as advanced as anybody. You've got the likes of a JPMorgan that creates its own code base quorum and puts it out in open source. The large financial institutions get it, they're focused on it, they're putting many millions of dollars against it, which is one facet of what you raised. The other is, there is a realization that for implementing blockchain-based systems in the traditional financial services space, the path of least resistance, and where the fastest progress is getting made, is where it works within the current business flows, by and large, and fits with the current standards.

There's a big focus right now, and we actually just put out a piece around HSM infrastructure. Hardened security modules, hardware security modules, as the standard by which current banks, from ATMs to the major systems running securities clearing. A bank's standard practice is to embed the keys, and the key management aspects, into a physical vault, a tamper-proof vault, if you even nudge it slightly in the wrong way, it destroys itself. It's a notion of putting keys into a physical vault, is the de facto standard that any CISO at a financial institution will tell you has to exist. So now, I'm working with a bunch of startups who have realized—they've realized all along but they've reached the stage now where they need to integrate and doing that HSM integration into a traditional bank's security infrastructure, in the traditional standard way, is really important and it's really hard, actually. There's a big focus on fitting the key management constructs into today's standard, as the first step. I think it will devolve from there, but it's a minimum starting point.

Demirors: Absolutely. Let's go then to the innovators. Melanie and Vinny, you're dealing with this every day. Both of you are in a sense trying to give people ways to manage their own identities, whether it's their physical identity, or in your case Vinnie, a lot of the data associated with their digital identities as well. As you think about your interaction with traditional institutions, about enabling people to permission-out their identity, enabling people to add components to their identity, enabling people to use their identity in new ways. How do you deal with the challenge of educating your users about the importance of managing their own identity. It really is a paradigm shift, right? I think people aren't used to thinking in this way about their identity in all the various aspects of their identity, as assets they should guard closely, and should manage like they manage the other parts of the assets they own. How do you educate your users on that and how do you get them to understand the importance of what you're doing?

Shapiro: Honestly, I think the NSA is doing that job for all of us. I think they're educating everybody, and I think that generally the media has shifted the conversation, and there's a lot of work taken off of us. I think a lot of people realize that they need to be in control of their data. The way that we—we're pre-launch, so at this point we're just working with partners for integrations that through them, we will reach our consumers. The way that we approach those relationships is very much that you as an organization don't actually want to control your user's data. There's an incredible risk to institutions when they hold all of this information, because if anything happens, whether it's their fault or not, their brand can be tarnished. It's going to look poorly upon their own security measures. The way that we look at it is basically in a pyramid, right? Where there are identity attributes, there needs to be self-control. Without self-control, there's no accountability. Where there's no accountability, there's no trust. The way that we speak to our partners is that we're ultimately trying to enable our customers to trust that you don't have enough power to control any of their information and you can trust that the system is protecting your brand or your company from having to be the next Yahoo. That's really the way that we're approaching it. To be honest with you, we've really had very little friction at the partner level, at this point. At the consumer level, I think it's all about eliminating friction. The problem with a lot of security measures is that every single time you add an additional layer of security, it's an added step or it's added time, and the reality is that consumers very rarely will prioritize security over convenience. That's why there's about 2% of Google accounts that have 2FA on them, which is ridiculous. These are people who have been hacked before and you still don't put two factor authentication on. The majority of people use one password across 20 websites and that's just because this model of security is a pain in the ass. To protect yourselves and use proper security, it's incredibly inconvenient. To be able to get to that point, we have to make it easy.

Demirors: Absolutely. Vinny, you have a similar sort of challenge, where you're going out and working with different partners, whether they're financial institutions, government entities, and working with them to participate in this new decentralized identity layer you're creating. As you go in and have that dialog, are you finding that people are excited by the idea of having users take more control of their identity, of not taking on that responsibility? Do you find that there's still friction or concern? What are the dialogs that you're having with your partners as you try to introduce this new paradigm?

Lingham: When we think about business, we think of it as a consumer data privacy company. We actually don't look at ourselves as an identity company. We think that identity is a subset of your data. How do we secure data and make it private? When we look at partners, there's really no incentive for them, often, to change. This is a problem with bigger companies. That's just the way it is, right? When you look at Google, for example, and two-factor authentication, we're at 2% right now with all the hacks, and everything else. I know some serious business guys that don't have a second factor on their email boxes, and these guys are running multimillion or billion dollar companies. It's very scary the way the world is, but there's a reason for this. The notion of two-factor authentication—Does everyone know what two-factor authentication is? Everyone? Okay, good.

Demirors: I think we saw a few say no, do you want to just quickly—

Lingham: Yes. Two-factor authentication is, for those of you who don't know, for example you have the Google authenticator app, where you type the code in after you log into your email, or you may have an RSA key, where the code keeps changing, and so you need an extra step. It's a username, a password, and then an extra code to get into whatever you're using. Your bank may send you a text message to login with a code, that's a second factor. The user experience is one which is in question here. Why do we need to have that second factor? Why do we need to have a user-entered password? Especially when that password is being used on all these other sites. It gets hacked one place, it's going to be used in other places, and they have bots automating access to multiple accounts. For example, if your username at Yahoo is vlingham@yahoo.com, and they will go—

Shapiro: It's not your username? [LAUGHS]

Lingham: Actually, I do have an old email. It doesn't matter, I have two-factor authentication on. If you have that, they'll go and use that username, and go checkout vlingham@gmail.com to see if the password works there as well, and that's how they get into your accounts. It's not very secure, anyway. The current metaphors we have around user access needs to be challenged. From a user experience perspective, wouldn't it be easier if you just had your identity on your phone, you could scan a code, and log into an app, or your banking website, or your email, no additional codes? People don't understand this stuff, so when you talk to average consumers—I mean, using a password was a big step for a lot of people 20 years ago, I mean a huge step. I think my dad hasn't gotten there yet.

If you change the paradigm of how systems are accessed, away from having to have the second factor built into the experience, I think we'll have more success there. For me, a lot of it is a user experience approach. When it comes to the companies, adopting these additional technologies, adopting easier frictionless methods, if that can help secure systems or make it easier, if their customer support level is going to go down, the risks go down, then they'll adopt it. But only typically at the point in time when they've had a breach or they've had some issue. Those are the challenges there. I do want to make one point on what David said early on, sorry to cut back here. As much as banks and financial institutions are investing a ton of money in blockchain, I don't think they quite understand it. There's two reasons for this. The first one is, a lot of the banks got together and started an organization called R3, where they pumped untold amounts of money into it, to build this blockchain-based system to compete with bitcoin, and whatnot. One of my most popular tweets of all-time was this, I said to Toshi Nakamoto, the guy who invented bitcoin, he created it in 2008 and released it in early 2009. The tweet was, I can't remember the exact words, but Toshi Nakamoto created bitcoin because banks didn't trust each other and the banks created R3 to prove it.

[LAUGHTER]

Lingham: R3 has really collapsed. They're not even using blockchain technologies anymore. The second reason is this, the best cryptographers I know, and the best cryptographers in the world, will never work for a bank or a major institution. These guys are like tinfoil-hat guys that sit in garages in Palo Alto.

Shapiro: David looks very sad now.

Lingham: David is—

Treat: I am one of these people. But I'm undercover at Microsoft.

Lingham: He's undercover, he's a mole.

Shapiro: You're not supposed to say that publicly.

Lingham: The majority of these guys don't work in these big banks, and Microsoft isn't a bank, so that's fair. Think about it, the bitcoin system was built as an attack on the banking system, to an extent. Then you have these vulnerabilities that come out, this is the problem with the banking system, and blockchain, and bitcoin right now. I just had my piece there, sorry David.

Demirors: I love this, bitcoin coming back in.

Lingham: He has a rebuttal if you want.

Demirors: Do you want to take a moment?

Treat: We don't have a lot of time left. I wouldn't count out R3 just yet. There are some pretty big court implementations underway, but you're right, they've taken a different technical path. I also wouldn't count the banks out yet, because if you look at the hiring profiles, we're actually seeing a whole bunch of those special people getting hired into them.

Lingham: Money talks. [LAUGHS]

Treat: Exactly. It's a huge focus and the banks have certainly woken up to the fact that if they don't invest heavily in this space, then they'll be in trouble. If you combine money and focus, things happen. I wouldn't—

Lingham: Not always good things. [LAUGHS]

Demirors: I would just add, as someone who is on the investing side and also working with institutions, I think the entrepreneurs do it on a scale of months and years, whereas institutions it's a matter of decades. It just takes a lot of time to shift the focus of an institution that's 100,000 people large. Maybe we'll be surprised.

Treat: I'd be more surprised, too. More and more banks are rolling out six to eight week cycles.

Shapiro: I don't know about that.

Demirors: We said it here, that's the best. We'll see you in a year. All right, so we've had a lot of discussion around digital identity, around security. I'd love to open it up to questions from the audience around what was discussed, things that weren't addressed. If you have someone specific you'd like to address it, let us know.

Johannes: Yes. My name is Johannes from Deutsch Telecom in Germany. Thanks for the great discussion. Let me add one special thing that is on my mind for a while. Let me do an experiment. When I come back to the US the next time and I'm standing at the immigration, I will ask the officer whether I can use my Facebook credentials to enter the country. Saying that, to me, identity is more fundamental than about entering a website or protecting my data. To me, at the very end, the state is in charge to guarantee my identity, independent of whatever technology might be underlying, but it's a fundamental issue that has to be done by the state to make it international. If the US maybe let me in with my Facebook credentials, I'll be in trouble in China the next day. Maybe this might be an identity or a guarantee that me, myself, and I are the very person standing in front of someone, that all your business model may be based on this in the future. Thanks.

Demirors: Melanie?

Shapiro: Let me start here. I can tell you that that's changing. There are groups of organizations and governments that are working together to make it a reality that you can move freely as an individual throughout the world on one system, starting there. The second is, if you are at all interested in identity, I highly recommend "The Sovereign Individual." It's an amazing book and it very much talks through all of this. You're right, very much right now the state controls your identity. In the future, we will have self-sovereignty. It's very hard to imagine that right now, but the types of things that we're working on put in the rails to make those kinds of futures imaginable and makes it possible.

Ultimately, the state should not have control over whether you are a person with an identity or not. Imagine people moving around from the Middle East, for example, and coming into another country. They're not coming to the US or Germany with any sort of passport or identity. Nobody is trusting those credentials and that's very problematic, as we see with our president who isn't letting them here. The reason is, beyond craziness, that we don't know who they are. We don't know if they're involved in any sort of illicit activity. In the future, we will be able to have pieces of information attested to you as a person, where you can walk into another country, and they have only what they need to know about you. I think the last piece of that I'll say is the best example I have is, my father-in-law emigrated as a refugee from Soviet Russia, and when he left, they left with nothing, as most refugees do. He has a PhD from Russia, came to this country, he basically has no education. That should be able to transfer. If he had control of that artifact, if you will, then he would be able to live here with the same degree that he had when he was there.

Johannes: What's your timeframe?

Shapiro: I mean, this is happening. We are live with a nation state in 2017. Is it going to be for everybody in this room? Absolutely not. Is it going to be for every country? No. But it's happening and that innovation happens, that's how it happens, step-by-step-by-step. And big companies, Microsoft is one of them, they're doing an amazing job to leverage the things they already have, the rails they already have to make a lot of this possible.

Buchner: One of those that's going to try and make that real, and this is still very formative phases. We're sufficiently motivated to reimagine some parts of LinkedIn. If you really look at LinkedIn profile, it's essentially self-attested data. You can't prove that you worked anywhere.

You can't prove Melanie's father-in-law's degree. We want to make that a reality. If you can imagine all these organizations and educational institutions having their own self-sovereign identity that stands for those institutions and being able to sign a proof and give it to you in a self-sovereign data store that you bare at any place in the world, not geographically landlocked, where that data about your identity answers to no one but you. That's where we want to be and we're going to try and make that happen.

Treat: Just another data point on the timeline. You're going to see all of the puzzle pieces that are required to do that, be announced and come together in weeks and months, not longer. The scale, the implementation, and the rollout is a different thing. But, the puzzle pieces are all going to be there in a very short time frame.

Demirors: I think that's the exciting part, that it's not just incumbents and startups. There are also regulators, institutions, academic institutions involved. I think there's a lot of exciting work coming. We have one final question that we have time for. I don't know if we have a microphone.

Natasha: Thank you. Good afternoon, my name is Natasha. From a security perspective on protecting our blockchain identity, what are your thoughts on implementing iris recognition software and fingerprint recognition along with the token keys for additional forms of identification? What are your thoughts on that?

Demirors: That's an excellent question. Biometric data for identity security, you look so eager, David.

Treat: It's a huge focus of ours. We have the leading biometrics platform globally. Like I said earlier, we've implemented most of the world's border control systems. Where you're using biometrics today, we've been helping to build all of that. We see that future in it, right? If your biometrics can be an attestation that are part of this and an interaction point, where your body is your body, or a device associated with your body, and the combination of those things, that's an enormously powerful thing, and it's starting to gain momentum. In a small but spectacular way, if you go look at MasterCard, which just rolled out the biometrics on card, right? First implementations, but that's going to go quick. To the convenience point, it's easy, it's insert, thumb, done. That's a beginning. Our phones, right? We've all gotten very used to our thumbprint opening the phone. I think that the whole notion of your body being that key and access point, is going to ramp very, very quickly. It's a huge focus of ours.

Lingham: One of the things which I'll disagree slightly on this, purely because I think it stymies the growth of the sector worldwide, because of regulations. The moment you're storing biometric data on certain citizens, it can't be taken out of the country, you have to have service locally. The rollout for these types of technologies is a lot more difficult to do when biometrics are actually captured and stored. If we're going to take that approach, it's going to take a lot longer than any one of us would like to see global identities being issued. That's the tradeoff, right? You can decentralize it, and you can do a device layer where, for example, Apple it's stored on your device. Apple doesn't store a copy on their servers, therefore the devices can float around worldwide and they're not breaking any laws. The moment you centralize the data on a server, and you try to take it out of the country, you're going to be— Those regulations have to change in order for that to be—

Treat: That's not what's going on though, those puzzle pieces together will undo that, because that is the problem.

Lingham: The problem is, when it comes to regulations we all know it's the order of ten years, five years—

Shapiro: We actually, for the past three years, have been developing biometric libraries. We've hired a team of scientists to do this for us. We used biometrics on our very first product and we felt it our responsibility that if we were going to use biometrics, then we needed to make sure that the way they were secured was better than what was currently available to us. Right now, honestly it's garbage. You either put your biometrics on a secure element or you have to move them to the cloud, that's really it. We've developed something really interesting, that actually enables there to be biometrics captured, and taken, without ever being stored. It's different than the way Apple's doing it, there's no need for secure elements storing, minutia points are never stored. That helps you move away from these regulations where you can use biometrics to move globally across the world and that's really, really important. You don't want anybody having the only ten passwords you have, because you can't change these.

Demirors: On that fantastic note are you all terrified about your identity data now?

Shapiro: Read "The Sovereign Individual," it's the best book ever.

Demirors: All right, so we're all going to go home and enable 2FA on all our accounts. Everyone should sign up for Civic, read about self-sovereign identity, watch for Microsoft's upcoming exciting identity announcement, and check out the great work Accenture is doing. Thank you everyone, I hope this was informative.