Blockchain at CMU and Beyond

featuring Eliezer Kanal and Eugene Leventhal as Interviewed by Will Hayes

---

Welcome to the SEI podcast series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally-funded research and development center sponsored by the US Department of Defense. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

Will Hayes: Hello, my name is Will Hayes, and I am principal engineer here at the Software Engineering Institute, a member of the Agile in Government team. Today, I am joined by Dr. Eliezer Kanal and Eugene Leventhal, who are here to speak with us about blockchain. Gentlemen, if you wouldn't mind, introduce yourselves and tell us a little bit about where you come from, what brought you to CMU and SEI. Elli, why don't we start with you?

Elli Kanal: Sure, Elli Kanal. I joined the SEI a little bit back. I was doing data science first at PNC Bank, doing data analytics. I went from there to Highmark health insurance company. I was working there also doing metrics and analytics, a lot of dashboarding. I came to the SEI. My team overall does data science mostly for the cybersecurity applications we have here: analysis of malware, binaries, and helping people do classification of that; analysis of insider threat data, and helping people find insider threats and the like. But my recent work has kind of gotten me a bit more involved in this blockchain technology. To that extent, here I am today meeting all these new people at CMU who do all this fun work.

Will: So there are a couple of threads from your past that we will pull in in a little bit, but let's have Eugene kick off.

Eugene Leventhal: Sure. By way of background, I was working in the consulting space in financial services mainly before getting here. I had seven years' total experience between my undergrad and coming back to CMU for my graduate degree, where I am currently a grad student now over at Heinz College on the public policy and management side. I specifically wanted to come to CMU because when I was sort of stepping away from the professional services world, I knew I wanted to go to an organization that was very active in the blockchain space.

When I started looking around, there was a short list of universities. I was very surprised that CMU was not on that list, but they had a very strong policy program. The policy program is sort of a data science light program as opposed to just being a pure theoretical policy program. It seemed the right pit stop, rather, along the avenue back to private industry before going into the entrepreneurship space. It seemed like the right both skillset and mindset to take on before jumping back in there.

Will: Great. As I understand it from a little background research here, you are trying to reach your arms across the university and really bring some focus on blockchain. Can you talk a little bit about startup and what you are working on there?

Eugene: Sure. When I came to CMU, it was actually pretty tough to figure out who was doing what in this space. Nicolas Christin has probably been the most active and for the longest time from the professorial side. He is someone who, I believe, released his first paper in the 2012-2013 time range. He has been looking at the space. I ended up taking his course in the spring. He was a great person to build a network with and build a relationship with, but it was so difficult to find the other pockets of who was doing what across CMU.

Elli and I got introduced probably about a year ago at this point. Aside from maybe two or three other researchers, it was very tough trying to find who else was even in this space at all. Around July of this year, I was put in touch with Michael Lisanti, who is the head of partnerships over at CyLab, and I was thrilled to hear that we now have an official CMU research initiative out of CyLab that is meant to do exactly what you just alluded to, which is centralize and coordinate. I know centralizing a decentralized effort is a little ironic. But nonetheless, at a campus, it needs to happen.

We are trying to centralize, and we were very happy to discover that we have over 30 researchers who are doing this, not just a handful. There are a bunch of private relationships of companies where we have people who are doing verification of private company algorithms and all these exciting projects that no one besides the researchers know about. So, it seems connecting those folks and building out the student community was really the first thing that I wanted to do and really needed to do in terms of having a more legitimate and more focused community here at CMU.

Now I am working on a startup with someone else here in Pittsburgh called Distributed 49. Our goal is to tie all the threads across Pittsburgh as a whole. So through the student activity side and with the research assistant job that I have over at CyLab, I am doing this officially at the university, but we really want to expand that out to the city as a whole. [We want to] find ways to collaborate with researchers outside of traditional academic settings and also to bring in

additional relationships beyond just executive education and the CyLab partners, which are sort of the two ways that we've been engaging in the past. So, we are trying to expand that.

Elli: We have had an interesting observation as this has gone through, that there is an enormous amount of interest from the student body in blockchain technology. It is really hot. You see this all over the news. You see it in a lot of startup funding that is coming through. You see it in the amount of venture capital that is going around. That is reflected in the population that we have here, so Eugene, being a member of a startup, is very much in line with what we are seeing on campus. I am teaching a course [Blockchain Fundamentals]—I am actually just starting that very shortly—on blockchain. I have never taught the course before, but just because the title is blockchain, the wait list is double the size of the class.

The students are super excited about it. There are certain topics where they are just trying to get involved because they see something as, *I can get a good job with it*. They are legitimately interested in, *What is this? Is it hype? Is it something behind it? Is it a niche technology that is going to eventually have a real good use*? It is the conversation. It is interesting to see that because all the professors are working on little parts of it, but the students, they are just as interested as well.

Will: So this is really a blossoming community, a blossoming set of topics that are really being rallied around this. So many people who have not heard of these more elaborate implications and applications might be thinking only in terms of cryptocurrency, that cryptocurrency defines what we are talking about. It is interesting to hear your backgrounds too, where you come from. You have business and financial industry backgrounds. But if cryptocurrency turns out to be the digital tulip that some people say that it is, blockchain still survives because of all of these other things. There is a lot more to it, right?

Elli: Right, blockchain has a strong relation to digital currency because before Bitcoin. That was one of the primary use cases where blockchain technology, before it was even called blockchain technology, was being applied. There's a paper, I think it is 2002, but the original was actually in '98 called Hashcash, and it was not exactly digital currency, but the fundamental idea was already being discussed there. There is a lot of push for currency because it just naturally flows, the concept of a blockchain passing around money, people. You can imagine how it works. Put the digital currency aside. Put all the ICOs [initial coin offerings] aside. The underlying technology is a distributed ledger.

Ledgers are present in many different types of business. There is supply chain. There is banking—forget the money, just the handling of the money. There is record keeping in all industries. You have licenses of all sorts. You have health data of all sorts. There are a lot of areas where this sort of thing could come into play. Not to say there are not challenges regarding

applying the technology, but there are a lot of places that it can be applied. All that said, there are a lot of technical challenges, and then the question comes up, *Is blockchain actually better than the current existing solutions?* And if it is, *What are the costs?* If it isn't, *Are there things that we can take and borrow from blockchain to either make the existing solutions better, or we can tack on these little bits and say we will use blockchain in this particular small part of the application?*

Will: As I understand it, the power of it comes from the massively distributed nature of it, from the fact that nothing is deleted. That you are not like my basement or my attic, continually accumulating those empty boxes, but there is really a sense of shared visibility. It is not unlike the open source community where sunlight is viewed to bring in higher integrity. Could you relate it in that way to open source?

Elli: Well, a certain extent because open source, when you have open source code. To give you an example, one of the biggest technologies that has enabled open source is source control, version control. You have, CVS, SVN, now we have GIT. When you look at what you have with these technologies, A) the code itself is public, and B) I can roll back to history. I can view history at any point, and say, *That one actually was the best one for me, because at this point something else is introduced. I am going to fork it. I am going to keep my own version and allow either the main technology itself to roll off to some other direction or whatever, however, I want to use it. I can look for small subsets and pull those out to my own code.*

Blockchain is actually very, very similar to that. I can look at history, essentially, its enormous state machine. I can take the state of the system at any time and say, *Here's where I was interested. I want to find something there*. As has happened a couple of times, I can go back to previous state and essentially fork the entire chain from that previous state as happened a couple times due to different hacks that have occurred. There is definitely a tie-in to that way of thinking. It has turned out to be an interesting complication.

Will: Some of the work that we have featured here before—your work on Obsidian, and your interest in trying to add more capabilities to this community. That is something I think CMU and the SEI are uniquely positioned to contribute to and your efforts across campus and CyLab. Can you speak a little more about that? What are the frontiers you are encountering?

Eugene: Actually, I would just like to add one more thing to the previous question. I also think it is indicative of a mentality that is becoming more and more prevalent. In terms of up until the'60s, there was no alternative to either government- or corporate-run projects of these forms. So at the end of the day, it is still new that technology can blossom outside of these environments. I think from a historical concept, it is really important to consider that we are roughly at the 10-year anniversary point. I think next Tuesday or Wednesday, whenever

Halloween is, I think it's technically the 10-year anniversary of the release of Bitcoin's white paper.

It has been 10 years since a mysterious entity released a white paper on a cryptography news list, right? It's very different than the runway between ARPANET and the other alternatives in the'60s through TCP/IP in the '80s and then browsers starting to actually be consumer-facing in the '90s. In my opinion—and I know I am not a technologic historian by any stretch—but this seems as though it's one of the first attempts to have a non-government or non-massive entity-sponsored technology takeoff.

And so in the last three or four years, we have seen more governments, we have seen more enterprises put money into this space, but I think the initial growth of blockchain similarly to the growth of open source and who are the kind of people to actually come home after a long day at work and contribute to the code online to never get repaid, it is this idea of, *There is a form of the world that we can achieve using cryptography and technology that is worth ideologically fighting for*. I think it is a small subset. I think the entire hype cycle and all the prices of last spring made a lot of people lose sight of that. I am actually really, but not my bank account, but all of the rest of me is very happy to see the current situation in the markets because it's kind of reminding people as to why you should care about blockchain. You are probably not going to become a millionaire by December. Let that go out the window.

Why should you actually care about this tech? For me, it was very much the idea of financial inclusion, especially for the two and a half billion people who are unbanked, who don't have any access to physical credit markets, to physical banks, anything like that. This is a way to leapfrog that step. They do not need to play catchup with banking. They can jump to mobile-based, potentially cryptocurrency-based, solutions that will be mobile. That was what first got me into this topic, and I am really excited to see where it goes.

Elli: One of the things that has made this such a fun relationship to grow with. So the way I first met Eugene was you reached out to me just to have a conversation. We sat down in one of the coffee shops around here and proceeded to have almost an argument back and forth about whether this is something worthwhile or not. It is funny because even this conversation kind of harkens back to it. I will let Eugene right now play the, *This is a huge proponent for social change*. You have actually given lectures on this concept. Blockchain is a democratizing technology, fundamentally. It used to be that banking was a centralized concept. Blockchain and Bitcoin specifically is democratized banking. There is no need for a central clearinghouse, which is a fascinating concept.

But when you look at the actual ecosystems that exist, that is the sole blockchain application that has really survived and thrived in the market. You have this concept of Ethereum, which is now

a public blockchain. And it has definitely been used as a trading platform mimicking Bitcoin, but the compute potential, the application of this as a distributed computer, has really not picked up so strongly. There are a whole lot of economic reasons why, and it is interesting to have those discussions. But it is interesting to point out, there is a huge amount of potential. There has simultaneously been a reticence to pick it up. It is interesting to figure out why and figure out, well, *How can we get past that?* If we can't get past that, what should we be doing with it instead because clearly, something is here.

Eugene: Going back to the question, the last question I just posed, it is interesting for me to see that perspective a year ago when I got to campus versus now and my guess as to what the market cycle has played into that. I think when I just got here there was so much reticence towards it. Everyone that I talked to was sort of, *Why are you wasting my time with this blockchain thing*. Even Nicholas Christin, who is really deep in it, was sort of *Yes, I understand*, a*nd here are the proven ways*. He still, I mean as a good academic, is worried about the ways that are improving or, thanks to what's going on in the market, that might be greatly undermined.

I was just coming at it from the pure excitement of, *Well, yes, isn't it still cool in this application*? *Shouldn't you just be excited about that?* Now, a year down the line, I feel as though that is totally reversed because everyone who was just in it for the hype kind of scoffs at blockchain. I remember doing my recruiting events around campus, people would walk by, *Ha, ha, the Bockchain Club*, and just keep going. Yet we had over 250 new people sign up and are one of the more popular clubs. It is this funny give and take on that side.

I think now why I am really excited about all these efforts and working with all the great researchers we have here is because applying more academic rigor while there is more investment coming in from the government, especially from private enterprise…Because I feel like there is a big disconnect between what private enterprise wants from a bottom line perspective, what is being sold to them, what is possible, and what is actually logical moving forward.

Going back to what Elli was alluding to earlier, a lot of fancy private databases are being called blockchains when they are just more complicated private databases. Probably trying to make them be a blockchain will make them work more poorly rather than just saying, *Let's just put in a distributed database and not go to this new fancy buzzword*. That is something that I would hope will diminish while we are seeing this kind of suppression in the markets. I think, which is why now is a perfect time for more academics to get involved.

The fact that we have 30 people at the cutting edge of either cryptography with thinking of two-factor authentication: you lose your private key, a way for you to actually get all your money back. That is a big one. People who are doing research on ledger manipulation, people who are

looking into better programming languages, whether obsidian or all their alternatives, different consensus mechanisms. Now we are starting to seriously think of all the little buckets that go into it. Now I think with the academic rigor across all of these topics, now we are getting to a point where the tech advance where we will see: *Are there situations where we'll ever need a private blockchain? Will private blockchains just be a thing of the past, and we'll remember the 10 years where Bitcoin existed as a funny joke and just move on?* I don't know. I think I am just excited to see people who are a lot smarter than I am working on this in a research environment and not in one where they are immediately, *If we don't make $10 million within the year, we are going to get canned*. I am really excited to see this different environment give sort of the space for people to plan.

Will: So with an undercurrent, this tension between centralized and decentralized—the joke at the beginning—you are looking to centralize the focus on these decentralized distributed technologies. If we think about, going back to open source again, Git is now an offering through Microsoft. It is how government organizations are getting access to that key contributor to open source. Are there things like that that are happening in the blockchain world where some influential authorities' decisions are actually opening it up for a wider array of people, probably the work you are doing and the teaching and research that you are doing? Can you comment on that?

Elli: There is a fascinating … it's a phenomenon where you look at it and you say, *This is a decentralized technology, but in order to apply it well we have to centralize it, right?* The concept of a bunch of researchers who are all doing something completely independently, we are going to put them in a building and have them call that building Carnegie Mellon University, is kind of an example of that. The fact that the technology is decentralized does not mean we will not benefit from centralization to a certain extent. There is definitely a distinction to make between what the technology represents. You can almost think from a philosophical standpoint, depending on how you are trying to argue it. But then *how do you apply it, how do you best apply it?*

One of the more popular blockchains out there right now, Hyperledger, it calls itself a blockchain, and there is blockchain technology underlying it. A huge amount of their architecture and their infrastructure in the whole solution goes towards centralization of the system. Without going into any detail, there is the blockchain aspects, but they specifically build in centralized components to ensure business flows smoothly. So you get some of the benefits of blockchain, but you will be able to get certain amounts of guarantees about your system that you would not necessarily get otherwise. It is always this give and take. But this is kind of what Eugene was just saying. When you start to think about, *Here is a technology*, and we're going to now say, *Forget the fact that we're rushing for VC money. Let's focus on fundamentals. How*

should this be applied? Where are the problems of this technology? *What are some questions that people should be asking that they haven't had time because they are so busy being focused on making a quick buck.*

Now that that hype has sort of started to die out, and we are getting significant research interest, we are getting some pretty interesting outcomes. The work that is going on right now on the proof-of-stake mining. So Bitcoin works by this thing called proof of work where you are required to burn a whole bunch of computer electricity in order to have the system run. You are paying an electricity tax almost. There is this thing called proof of stake. How it works, don't worry. But fundamentally, it is a fascinating piece of technology. The people who are thinking about it and coming up with it have accomplished something really, really unique. It is a fascinating advance, just to read about it: *How can I get everyone to agree on something, you know, a very constrained system?* You are seeing some real advances here. They are trying to push us forward and say, *Now we can make this be more broadly applicable used in a better sense*. And it is very cool to see.

Will: In some sense we are hacking the notion that centralized, closed down, exclusionary equals safe. We are now kind of broadening it to understanding what safety and security is about with a completely different perspective.

Elli: One of the things I would take on that, it is interesting because when you look at the Bitcoin network…You said before, you cannot delete anything off of it, so that may be a huge benefit to someone who is attempting to perform an audit. But for the person who had secret information somehow attached to a transaction in the Bitcoin network, and this has happened, that may not be such a great thing. The whole GDPR [the European Union General Data Protection Regulation], which just came out of Europe, that concept includes the right to be forgotten. Is blockchain fundamentally incompatible with this concept? If it is, is there any way we can re-include it? Is there a technology solution which you can apply to that?

One of the lectures that I am researching in this course that I am giving is legal aspects of blockchain. It is interesting because one of the earlier papers—right now it is all legal theory, there's actually very little applied—one of the earlier papers argues blockchain is essentially the most vulnerable way to structure any organization. Because everyone is maximally exposed from a risk perspective, and there is nothing put in place to make sure that they have any protections against fraud that occurs in the network. And we have seen this.

I am forgetting all the names of the companies where this happened. There was a company that had a huge hack, and so the way they responded to this hack where they lost a huge amount of money was they gave every single participant in the entire network a haircut. So all of a sudden, everyone lost 36 percent of their holding. That is not necessarily something you want to be

involved in. Or maybe it is, because you say that is the benefit, and in the long term it will be a more stable network. But it is interesting to see how something that will be a benefit in one case doesn't always play our so nicely elsewhere.

Will: So some amount of what we heard as children, *This will be on your permanent record, kid!* So adding caveats to your permanent record doesn't really take away the pain and the sting of what was there before.

Elli: Very much so. In many situations where you have a record currently, whether paper-based or computer-based, it is implicit in the system, there is a way to remove that record. If someone has a particular piece of medical history, which they don't really want to have in their file, they can get rid of that. It is up to them as a patient, or depending on who is in charge of the file system, to get rid of that. Under blockchain, there has to be a technology solution to enable that. Depending on how you implement a system, you may or may not be able to accommodate.

Eugene: I know certification is a use case that's come up, the idea of proving that I have either accomplished certain knowledge or attained certain skills. But even so, a lot of those systems that are theoretically drawn out are predicated on the educational part being all automated and digitized. So there, it's much easier for you to understand, *Did I learn Python to a certain degree because you can review all my course studies and everything*? But if it is say, public speaking skill, and it needs to be assessed by a human being at some point, then that is an inherent vulnerability in terms of proving the authenticity of the information that is there. What if you are the person transcribing my ability. You just accidently confused us to you thought, *He's great, I'm not.* You put something wrong down. Well how does that get changed, because in my record, all of a sudden, it says I am a great public speaker? With something so innocuous, yeah, most public blockchains don't have a solution.

The private chains that will offer opportunities for ways to do that, a lot of the time, the more, let's say the purest, especially the Bitcoin maximalists or whatever you want to call sort of the folks who have been ideologically in this since the beginning and are very much saying that Bitcoin still has a place in society, which is something I do believe in. But they will look at any of those attempts and say, *Well then you are just making a fancy database because you are stepping away from the immutability, which is the exciting part of a permission-less blockchain*. And so it's just this never ending back and forth. *Well, that's great, but how do you actually solve these problems*. And they do not have an answer to that.

It is a bit frustrating, but I know zk-SNARKS is one area that I'm super excited to see, which for the listeners, is sort of a form of cryptographic primitive where you can prove that something has happened without actually needing to prove that thing itself or show any identifying information. Just think of it as sort of a verifying algorithm on top of whatever you are doing.

It's a horrible way of putting it, and I'm sure if the founders heard that they would yell at me. At a rudimentary basis of why you should care, I think that at least captures the gist of it. But that will be huge, because that will be game changing in terms of what information should or shouldn't be on a blockchain, because if you can truly anonymize it so to a way where only encrypted information gets up there in the first place, it's OK if no one can decipher it, as long as someone can still prove that even though no one can read what is in this hash, we are verifying through this algorithm, which we will have to trust at some point that it is doing its thing. But the matter of trust is always a tricky one.

Will: So you keep pushing me back to thinking about open source. What happens if we have malware out there on a very commonly used component that is all over GitHub? How do we remedy that issue?

Elli: This is the last one I remember. I am sure this has happened since then, but there was a very well-publicized incident where a user deleted a particular library off of NPM, the Node Public Library. That particular library happened to be used in a webserver, so that as soon as he deleted it, some 30 percent of node-powered websites just died immediately. It is one of those, *Dude, not cool!* How do you fix this?

I'll go even further. There has been a lot of discussion about using blockchain technology to propagate—I'm going to get this wrong again. Guys who are going to listen to this are going to yell at me—name servers, DNS systems that underlie the entire Internet. All we are doing is propagating records, and we are showing record updates. Use blockchain for that.

There's been a lot of discussion about using blockchain technology underlying PKI [public key infrastructure]. If I'm going to put out this public key, here's a great system for it. It's distributive by nature. The whole goal is to have this information get out there, make it this way, and put out the revocation records the same way, but it all comes back. You are totally right.

And this is an area where there's a lot of cool research going on. You mentioned before Zk-SNARKs, that's CMU research. I'll just poke our flag here. There is a lot of cool research going on, and people who are trying to figure out this exact sort of thing out, how can I both have the benefits that I could gain, and simultaneously enable technology, or enable policy that requires me to not have something, which is fundamental to the technology. There's no good answer yet.

Will: Yes, how would we enforce such a policy, right?

Elli: Right. There is no good answer yet, there is really no good answers. It is part of what makes this such a fascinating field. The entire field of blockchain starts 10 years ago. And when I say starts 10 years ago, there were maybe 100 people who knew about it when it started. We are talking *started*. It got popular seven years ago, maybe eight, depending on how you are going to

define popular. This is a nascent field. This is not something you get to see every day. You are watching this new technology spread out. Unlike something like a tablet or an iPhone where the same concept applies, but we are just seeing it grow. So, *I understand the phone, I understand the computer, I have a phone, that's a computer*. Cool, I can marry that in my head. Blockchain does not have that similar model that most people can go to. For people who are programmers, I can point to Git and say it's kind of similar to Git with some caveats. Most folks don't know what Git is, and it requires a full paradigm shift in their head to say, *this is a computer that's simultaneously running on everyone's machine at once, and no one has to keep track of what it is up to because that's the whole magic behind it. And by the way, it doesn't forget anything*. And it also knows who you are because of ID and PKI and all sorts of fun stuff. I've never heard of that before. And just explaining it and figuring out the new problems with it and figuring out how it fits in existing policy is a challenge.

Will: And does this someday lead to things that Captain Kirk and Mr. Spock enjoyed. They don't have to carry a wallet. So there are things that are so ubiquitous and so common, we don't need that hiding place that we keep in our hip pocket anymore.

Eugene: There are already places around the world where you don't really need to carry around a wallet anymore. In China for example, so much of it is mobile based through Alipay and through WeChat, you can cover so many transactions between friends plus buying regular things, plus hailing a rideshare with WhatsApp, all in one front, so I think there are definitely places across the world that are already showing us a little glimpse of that future. But piggybacking off of what some of the things you are just saying, I get really excited also by the idea of distributed governance. If you have a truly decentralized network, where does the governance come from? That is a whole new mess that we are starting to deal with on larger scales. And each time someone plays around with it, everyone from the outside will say, *Well look at that mess. Why would we want that?* But then if you get a group of more than two people together and you need to come to a decision consistently in things you do not necessarily agree with perfectly, it is not easy.

The way of systematizing that I think is key especially for some of the more open permission-less systems, if they want to be as global as they claim to be. I think at the very least it is forcing us to reconsider, *How we are transacting things of value. What are the things of value that we're transacting in the first place? We are seeing that a lot of them are digital*. And in this environment where more of it can be automated, *Where you need fewer people touching it along the way, how can we create forms of trust and agreement between them*? And that is where it's such a difficult challenge. And I feel the first sign of a person not really getting the benefit of Bitcoin and consequently everything that's come since is when they just kind of gloss over it as if it's this inconsequential thing.

Even if Bitcoin disappears tomorrow and proves to be totally wrong on every assumption, then the Nakamoto consensus and the advancement it gave from a distributed-consensus perspective is a big deal. No one's been able to achieve that. Paxos Raft are the ones that tried to do it in different ways, but no one's done this in this truly open fashion. And even though it is still not the most efficient thing in the world by any stretch of the imagination, that still might have a role to play.

Last week I was having a discussion with someone and they were asking me, pretty confrontationally, *Well what's the point of Bitcoin?* In the context of the U.S., I was trying to explain, *Don't think of it here, because all of the analogies fall apart. Think of it in a place where you don't trust your government. You don't have access to a bank. You do have a mobile cellphone. You do have cellphone and mobile technology*. And all of a sudden, a lot of these things started becoming a little more clear. I think it's also important for entrepreneurs or anyone who's thinking about the space, don't just think about the environment you're in if you are in the U.S. or the West. Think of the areas that have the biggest problems in dealing with certain topics and try to think of how a tech like blockchain can help in that environment.

Elli: And jumping off that, because I think, still it's worth going into a bit more. The concept of Byzantine fault tolerance, so what does that mean? What it means is I can have a bunch of people who can't talk to each other. The environment in which they live is actively adversarial. People are trying to disrupt their communications, and they can still come to a consensus about a decision. That is an advance. That is not something that is trivial. How do I get all these people to come to an agreement about something when they can't even talk to each other easily? Fundamentally that is a huge advance.

You were talking before about Zk-SNARKS. Zk-SNARKs is a way for me to prove something to you without you even knowing what I am proving. There is some magic, something happened in my hand. I don't know what it was, but I can prove to you that according to some rule set, *this thing is true.*

In the abstract, it is kind of hard to imagine what that means. Here's what that means. That means I can say, *You transacted with you. In fact, I don't even know that it is you. I don't know that it is you. I don't know how much money you had. I don't know what the nature of it was. But I know that it happened, and there's a public record that this happened*. Now abstract it up. *I know that two companies did business. I know that this person has a license or a license was issued for something*. The person will be able to claim it at some point using some form. But broadly, there is evidence that this happened. That concept is so foreign to us because we are so used to saying, *Show me the evidence*. Well, the evidence can now be given without anyone giving up privacy. That is a huge advance. It is such an advance that people listening right now

are probably thinking, *I don't even know what that means*. But the fact is, this is now possible. I can prove that something happened without having to tell you anything about what happened.

Will: That can be kind of disquieting for people who are accustomed to having a greater level of verifiability. Understanding that something happened means *understanding* it.

Elli: Very much so.

Will: But the way you guys talk about this, it's almost like this evolution is inevitable. That we will all be leaning into this before we know it.

Elli: Let's go the other way, right? It is now public on YouTube—and I encourage anyone listening to this to go check it out. It is almost trivial for me to make a fake video complete with audio of someone speaking. I can just put their face on top of an actor's face. I can mimic their voice using computer technique. Now they are speaking the word that I want them to speak using their image. That did not happen, but it is right there.

So the concept that we have historically of, *Show me, let me see it*, that is going to have to go. We are only now seeing how important it is for that entire mindset to really start going out the window. As we move away from that, we are going to need some way to say well, *What is the proof then?* This doesn't give us a way to give the proof, but it definitely gives us tools that when we figure out what the proof is, I can convey it to you. I can not only convey it to you in a way that you'll believe it, I can convey it to you in a way that you will believe it that I don't give up some privacy that I might have to do.

Will: That is a 180-degree turn from, unless it's been on social media, it didn't happen. If you don't see the picture of the great meal I had, I didn't enjoy it.

Elli: Exactly. And it's definitely going to require an increased level of sophistication from people who were using it. And by sophistication, I mean they're going to have to understand, even though I don't know what all the math is behind this, I can appreciate that this is now representing truth. The math gets a little bit hairy. I only know that because I tried to have one of the grad students explain this to me. And it is hairy, I am not going to lie to you, but it's very cool. The fact is, this is where we are going to see proofs and the concept of verified evidence, validated evidence going in the future.

Eugene: I just want to add one quick thing. Stepping away from text specifically, I think what both blockchain and other technologies are forcing now to some degree that is a bit unprecedented is the amount of personal change that is necessitated. Because we are no longer talking about being a user of something, we are envisioning products that fundamentally require humans with different values and behavioral programming. And we are just not there yet. So, the

idea of my own understanding of personal responsibility, that is something that has to evolve. The idea of managing and living through ambiguity, that is something that most people will pay as much money as they can to avoid, ambiguity.

We are moving toward a world of guaranteed ambiguity, guaranteed consistent digital threat of someone's trying to break through and hack us somewhere from somewhere. In this environment, we still keep continuing buying into a lot of these convenience apps that make it seem as though, *Oh you don't have to focus, you don't have to take on*, because automation equals you do less. Well no, automation means you can do some of the mindless things less. You can still be cognizant of them. It does not give you a carte blanche to not care anymore. You have to still be the captain of your ship so to speak. But that's one thing that I see as a huge bridge between tech and just humans. That is one that I actually don't see anyone really trying to bridge, and that is why I wanted to come to policy school was to take a different approach than everyone else is doing, what would have done in my shoes, which is MBA and then to a startup. It's not as though I know the right answer. I don't think anyone has the right answer now. I think it's more of, it's a good thing that more people are complaining that this is a problem to begin with, which is already a good sign that at least people aren't alone in their thinking. But yes, that's a much harder one: *What are the behavioral economics necessary for technology to get the social change necessary for that tech to take off and work?* I don't know.

Will: This has really been a wide-ranging conversation. You talked about the whole world. Let's talk about one really special place in that world, and that's Carnegie Mellon University where we all live and work. What is going on here that we want to make sure we leave the viewers with?

Elli: Within the Software Engineering Institute, it's actually kind of funny, we don't have a huge amount of focus on blockchain historically. Where we are going now is two real aspects. The first is blockchain security. I am a member of CERT cybersecurity. We want to make sure that the blockchain itself is a secure environment in which people can operate. Turns out, that is difficult to do.

We've talked in the past about Obsidian, and we will continue to talk more about it, but the briefest of explanations is that right now, it is very hard to program. If you are going to make a computer on the blockchain, it is really hard to program it in such a way that it is actually going to do what you want it to do. It is very easy to screw it up. So we're making this blockchain technology where you can code on a blockchain and keep it secure, have a guarantee, or at least have some more guarantees that what you are coding will actually do what it is intended to do.

The second area where we are getting pretty involved is advising government. There's a huge amount of, I don't want to say misinformation, but confusion. As people are trying to learn more what blockchain is and they see these different sporadic use cases come up, and 9 times out of 10

the use case is really not a great one, it gets very hard for people to understand, *What should I be doing with this? What's a good use case?* We are trying to play that role of trusted adviser and explain, *All this other stuff we've talked about before notwithstanding, here is where you're probably going to want to focus based on whatever your interest is. You know, if we're talking to this department, to that department or this whatever, here's where you would be interested in.*

Will: So reasonable on-ramp, a reasonable set of choices to limit yourself to until you get much more capability.

Elli: A lot of talk about pilot studies and about what small area we could shoehorn this in. Also, a lot of talk about how do you integrate this with existing technology. Blockchain does not naturally fit into a software ecosystem as it exists nowadays. We have the model of a database holding all the information. You do not want to just carte blanche go onto a blockchain, because of what we were talking about, about permanence and about policy and requirements. But at the same time, you want to make sure that however you are using the blockchain, you are getting some benefit from it and you are not just putting junk data on there just because now you are using a blockchain. So figuring out that balance and that scope is a pretty big challenge.

Will: So you don't just knock down firewalls and make it massively distributed. You transform the concept of firewalls to a different kind of trusted environment.

Elli: Sure, and again, blockchain is a technology for running things and storing things. But a lot of the traditional security aspects still apply. For example, if you are storing data, that means the data is there to be accessed, which means it can be accessed by someone who you don't want to have access it. Sure you can have all sorts of cryptography, but you can have cryptography in traditional databases as well. A lot of the historical concepts abound: network security, secure architectures of entire systems, permissions in accessing, all that frequently still applies to a blockchain-based application as well.

Eugene: I will quickly tack onto that, I remember I went to a DTCC Conference back in 2016; it was my first sort of foray of getting more active into the space. I remember hearing a senior banking technologist come out and say, *Look, we appreciate all of you brilliant coders out there who have never worked a day in finance in your lives, but you have to understand that we are not all getting rid of our tech stacks. No matter how powerful blockchain is, we're not throwing away 50-plus years of financial investment.* And you could just see the eyes of certain people in the audience open up of, *We never thought about that*. It was funny.

Elli: *We have got 50 million lines of COBOL. It is really not going away tomorrow, and however awesome your stack is, it is not 50 million lines of code.*

Eugene: Yes, I remember the big takeaway that day was, *On and off ramps, not replacement, people, on and off ramps.*

Will: And Iron Mountain will continue to have paper stored. Those are old habits, or are they good practices? What do you think, guys?

Elli: We are going to see. As we move towards more and more digital and all the risks we were talking about before, there is going to be a lot of paper.

Eugene I just heard, in regards to voting, there are a lot of jurisdictions that are bringing up the question, *Do we bring back paper ballots?* How can we verify the votes in the first place, purely for audit? So it's interesting how we might end up coming full circle to, oh we are digital, it's just backed up by paper. To tack onto what Elli was saying in terms of some of the great things going on here, I also just want to mention that CMU has become one of the leaders from a class perspective. There are four classes that are fully dedicated to blockchain. Two of them are full-semester classes taught out of the School of Computer Science, either by Nicholas Christin or Vipul Goyal. Elli mentioned that he is starting a class today. He's one of the half-semester courses that we have going on. And the other half-semester course is taught out of CMU Rwanda, which if I am not mistaken, was the first course at a university on the continent of Africa to teach a blockchain-related course.

Here in Pittsburgh, we have another six classes that touch on blockchain ranging from distributed systems to more of a network forensic-analysis class, to more of the economics and financial markets perspective, with a fin-tech class and a financial crises class, and then some more pure technology ones. And all those range from a single class to a couple weeks being focused on, as we have been talking about, 30-plus researchers, most of whom are doing a good portion of their time dedicated to blockchain, ranging in topics from scalability to security to more of the usability side to some of the pure economics. We have some folks who are starting to look at it from more of a socioeconomic standpoint, which is very interesting. So yeah, I'm very excited to see the fact that we're not just driving it from a cryptography and computer-science perspective. We have every school on campus pretty much with the exception for now of CFA, the College of Fine Arts. But we will be putting on a blockchain play, Spring 2019.

We are getting a lot of students involved in seeing both from the undergrad, graduate, PhD. We have some professors coming out who are really trying to see across the gamut. And we are excited to try to get more group projects going. We have had a variety of startups come out. We have had Zilliqa from Singapore last week. We have Hollow Chain coming through next week. We have Air Swap, which is a decentralized exchange later in the year. We have Republic Crypto coming out. And we have about three or four other companies that we're talking to.

ON the club side, our goal is to create a pipeline ranging from, *You have heard about this and you want to learn a little more*, all the way through to, *I am knowledgeable, and I want to get a job in the industry*. We want to be able to cater to folks across that full gamut. And that includes pitch competitions. That includes general education, professor showcases, research showcases, student presentations, workshops, technical workshops as well. We are really trying to make a very active community.

I think CMU should be up there with MIT and Stanford and Cornell and a few of the other ones that have already claimed a name in this space because they have been in it for so long. I think CMU should be up there with those folks. And hopefully, the work we're doing through CyLab and through great folks like Elli will get us there.

Elli: It is worth mentioning that you are doing stuff with Pitt [University of Pittsburgh] as well. I mean, this is a Pittsburgh effort not just a CMU effort.

Eugene: Yes. I know when Hollow Chain is coming through next week, we are coordinating with the Pitt Club that is going on. And I am going to be reaching out to Duquesne and Chatham and to the other major universities in this space, and we have been working with professional developer groups. So we are really trying to make this Pittsburgh-wide, not just our great little community and our little CMU bubble.

Will: Eugene and Elli, great. Thank you very much for all this neat stuff. And if you are seeing this, you have access to everything they have just mentioned because you are looking at something coming out of Carnegie Mellon University. Thank you for joining us.

This podcast is available on the SEI website at sei.cmu.edu/podcasts and on Carnegie Mellon University's iTunes site and the SEI's YouTube channel. As always please feel free to reach out to us with any questions you have at info@sei.cmu.edu. Thank you.