Cross Chaining the Future With DLT Gateways. Dr. Thomas Hardjono, CTO, MIT Connection Science & Technical Director, Trust-Data Consortium

[00:00:00] Eric: This week, the encrypted economy had Dr. ThomasHarjono the podcast. I probably could've done a few different podcasts with Dr.Harjono I was drawn to his current paper on DLT gateways, and thus this podcast, I've been reading a lot more papers lately. I hear a lot about TLDR, but generally I am a TSDU or too short didn't understand.

Anyway, Dr. Harjono was a driving force for years behind the MIT Kerberos consortium, which is probably the most ubiquitously deployed symmetric authentication protocol worldwide. He was an engineer at Bay Networks, a principal scientist at Verisign PKI and in a number of startups as well. He's an authority on identity, data, privacy trust applied cryptography and cyber security.

Fundamentally, one of the problems that he is trying to solve for is interoperability between DLT networks, which can be private networks in his view, the DLT gateway, he [00:01:00] discusses isn't necessarily competitive with bridging networks like wan chain.

He views standardization of DLT gateways as complimentary to bridging networks. In many ways, I could see how this standardization would facilitate more bespoke, private DLT network implementations, and then that could facilitate even creating networks of networks.

Gateways can facilitate common standards across multiple protocols. And thus achieve interoperability. The gateways themselves are not the cross chain solution. They need another protocol operating in between the gateway. One of their target use cases is a bold one facilitating interconnectivity of virtual asset services.

Providers VASPs as envisioned by the Financial Action Task Force. In that context, one acronym that pops up is Theresa T R I S a or the travel rule information sharing Alliance, which he speaks about on this podcast. There's an also, [00:02:00] there is also an interesting sidebar in here related to the architectural decisions, underpinning the development of web two O and decisions that student away from more of a web three O implemented.

And there are a few acronyms. I want to touch on that. Pop up during the podcast. Um, they come up a lot. So maybe you should pay a little more attention. Now there's a few acronyms. I just want to bring you up to speed about there's a few acronyms. I want. There's a few acronyms I want to touch on before we get into the podcast because they pop out.

The light one is ODAC. This refers to an open digital asset protocol, which is a protocol that can operate between two gateway devices that Dr.Harjonowas involved in creating. But it isn't the only protocol that can operate between gateways. Another one is IETF. The internet engineering task force, which is a large open international [00:03:00] community of network designers, operators, vendors, and researchers focused on the evolution of internet architecture and the smooth operation of the.

His paper has been submitted for publication as a standard of the IATF, which means that it would have completed a rigorous review process designed to identify any open engineering issues. So at that drop, I bring you this week's episode with Thomas Harjonoalso, if you like this podcast where you think, you know, others, that would like it, please share it.

So we're with Dr. Thomas Harjono uh, currently the CTO of connection science and technical director of the MIT trust data consortium. Welcome Dr. Harjono.

[00:03:44] Thomas: Thank you, Eric.

[00:03:47] Eric: Um, so, uh, before we get into the podcast, maybe give us a little bit about your background and, um, what brought you to looking at, uh, I guess gateway mechanisms for public blockchain and [00:04:00] blockchain generally.

[00:04:02] Thomas: Great. Thank you. Uh, Eric again for having me on this podcast. So, um, I guess I am a child of the early nineties and, um, grew up through this whole, uh, internet revolution when, when TCP IP was not yet the CPIP and when the IP packet data structures were still not finalized. And, um, you know, so, so this is, this is I see parallels.

Today's world of, of blockchains and crypto and so on. And I think this is an exciting time. Um, and I wake up every morning thinking, wow, this is, you know, I'm living this twice over an hour. This is, this is pretty cool. Uh, so a bit about my background. So, uh, in the early nineties, of course, um, you know, uh, a number of companies, startups were developing, uh, solutions for IP routing.

And my first early job was in fact with a company called bay networks, which is now been [00:05:00] forgotten at the time. It was actually larger than Cisco and you know, it occupied, you know, 60% of the market. And, um, in that, uh, in that period, my focus has always been security. So IP security, uh, IP multicast security was a big deal back then.

And of course in those days before the iPod, the first iPod came out, it was all about DRM and DRM, uh, you know, data, uh, content protection. Yeah. And I moved on to the area of, um, X 5 0 9 digital certificates, which is essentially publicly, uh, uh, public

cryptography. Uh, and, uh, that was also deemed to be very crucial technology and today with, you know, with Bitcoin and so on, suddenly there's a Renaissance of interest in cryptography, particularly in public key type, you know, cryptography.

Uh, so I spent a few years there worked for a company called Verisign and understood the importance of, uh, services that provided public [00:06:00] key related, um, you know, functions, particularly for certain verticals. So the one I was very familiar with is the cable network industry, because back then kids used to hack the set-top boxes with the goal of getting free movies.

And the whole industry essentially moved over two or three years, uh, into this, um, Uh, device certificate model where you're in a setup box would have a certificate. And the network provider upstream would have the CMTS SIM test server, which is run by the cable provider would have the same thing. And so on.

Uh, uh, from there, um, I did a couple of startups, got burnt out and ended up at MIT, uh, running the Kerberos development teams. So Kerberos is an authentication protocol that originated from a 19 82, 9 84 paper. This is the famous Needham Schroeder. Uh, protocol, uh, those are big names for those societal [00:07:00] cryptography.

That's probably your lecture one week one, you know, symmetric key base authentication, which is kind of interesting because it's not publicly based. And so, uh, Kerberos was a core part of the famous MIT project, Athena that included different parts, such as the X windows, for those who remember X windows, that is the grand grand daddy, daddy, or what we have today in the computer, which is windows on, on the PC, on the Mac and at MIT, um, you know, people wanted to share resources such as files and file systems.

And there wasn't, there was no authentication protocol. There was nothing. And so. This project started way back when, and, uh, when I took it over, you know, um, back in, what is it now? Uh, 2007, you know, we were trying to find a way to move the code forward because what had happened was the code actual software had been included, embedded within [00:08:00] products, such as active directory, which is the Microsoft flagship product.

And therefore, basically any. Um, company and enterprise, it runs Microsoft of any version, you know, client and server would have our code in there. And so Microsoft has done awesome. Beautiful work on top of the Kerberos has got, has got amazing, amazing, um, features that we could, we need this special podcast is to talk about the features of, of Microsoft Kerberos and of course, uh, Mac of, you know, um, you know, is on Kerberos as well.

So that was part of, you know, our achievement MIT was, you know, during this five, six years that I was leading it, we had a whole bunch of companies come and say to us, like, what features do you want? Right. So, so that was, uh, the MIT Kerberos foundation and the Kerberos protocol development is still running.

It's still ongoing. It's. Primarily done through, um, you know, emails and, and so, um, I've stayed on a MIT to the [00:09:00] addictive place, as you know, this is so much going on. And, um, you know, back in 2000, I think, um, eight or nine, I read this, uh, you know, in the Nakamoto paper and kind of, kind of yawn, okay. Like this is, this is beautiful.

This is beautiful work, you know, three different pillars of, of design of construct supporting this currency. But Hey, you know, I was, I was around when Digicash people might remember, did you cash withChaumway back? And I was excited back then and it was, uh, it was, I was disappointed. Okay.

[00:09:35] Eric: I'm not going to get burned this time.

[00:09:37] Thomas: Yeah. You know, and like, oh, what happened? Digicash didn't go anywhere. But the credit card industry did the card payments industry. You know, blossomed in the last 20 years. And so I said, okay, yeah. Okay. And I Bitcoins. Yeah, that's nice. But like who would use a Bitcoin for goodness? You know, a little little did I know that, you know, I paid attention and of course I think for me, the, the, the, the real sort of meat [00:10:00] of, uh, was when, um, Ethereum came along with the smart contracts.

Right. It's okay. This is a very interesting construction. So we've been looking at that. So back to your question about gateways, um, the internet design, um, of, you know, of the eighties and nineties also faced the same dilemmas that we had local area networks LANs that employed specific, not just specific cabling technology, but specific packet data, packet, structure, technology.

And so how do you interconnect these networks? Um, there's a thing called, you know, border gateways that are using the internet today. So the same architecture, uh, you know, it's kind of where we're visiting the same architecture for the purposes of, of, um, blockchain and blockchain network, interoperability and crypto.

[00:10:51] Eric: And so moving out of the, I guess, you know, we're, we're, we've been in sort of the hype cycle stage, which has generated a lot of attention [00:11:00] onto crypto, but as we start to move out of it, how do you anticipate these lay a layer one, uh, public blockchains evolving from here?

[00:11:10] Thomas: Um, a very good question. This is actually one of the motivations for.

For gateway. So, so, um, when we looked at gateways, uh, we tried to undersell it. So first of all, why did we have this CPIP to begin with? And for those who are interested, um, one of the big names, you know, so modern, like the heroes of mine, you know, there's been surf and Bobcat, and of course there's, there's, uh, Dave Clark at MIT.

Dave Clark's got a nice new book, I think last year or year before on, on the history of making the internet. But, but the motivation back in the late sixties was the fact that the United States communications both. Uh, civilian and defense was based on this connection oriented teleco model. So the theory was that it, you know, in those days, the cold war, remember the enemy could just whack would just bomb in a couple [00:12:00] of phone, major phone exchanges, and we won't have any communications right into it.

So, so this whole routing model was developed and, um, in, in, uh, so, so in, in Jose's that the, you know, just telcos was like one company, right. They, you know, at and T told us what the packet, AT&T told us, everything, right. Find that word for a time. Now I, you know, this whole gateway model is trying to address the same problem that you have, um, a proliferation of these, uh, networks that essentially hold assets.

Right. But then there's this problem of asset mobility and survivability. So another big event, I, you know, that, that people, I think sort of gloss over it was the CryptoKitties. So CryptoKitties. Placed the Ethereum network, almost at a standstill it's sort of halted. And this brought the question of survivability because back in the sixties, the reason why DARPA and the [00:13:00] army and so on plays so much investment in the internet was certain communications survivability.

So today, do we have equivalent survivability? If, if tomorrow there was a day zero virus that crippled, you know, 90% of all the mining nodes, you know, uh, forging nodes, thinking nodes of a network. My asset is stuck there. I can't move it out. Right. So how, how do, how do you solve this problem? Because for investors don't want to know about this investors that say, if I want to sell it now, I expect that the it will be settledd in the next five seconds.

I don't want this business about, well, gee whiz, we've got, uh, you know, blockchain, uh, overload and the transactions are very slow today. It's like, it's, it's not, you know, that's not acceptable for, you know, the today's sophisticated traders in wall street.

[00:13:54] Eric: Right, right. Um, and do you see a proliferation of more layer, one [00:14:00] blockchains, more private blockchains?

I mean, I guess you could say both, but do you think there'll be a consolidation? Uh, probably not so much among private blockchains because those I think would just continue to proliferate. But do you see a consolidation against layer one blockchains or do you think we have a long way to go still before we get to that

[00:14:18] Thomas: point?

Uh, that's a, that's a good question. I'm. I eventually there needs to be consolidation. And then I think just, just sort of just human beings have a limit to how much complexity our brains can handle. Right. And at some point in time, we'll all say, okay, enough, although this, you know, different variations of a blockchain let's, let's, you know, set a lot of like three of this, a small number, uh, with, you know, in-built functions that are relevant for, you know, certain types of transactions.

And what will happen would I think is the same technology that's used in the public networks will just be adopted inside private networks. It's just easier because [00:15:00] you know, if you're an enterprise or your consortium and enterprises, you know, you just want to buy software and run. Okay. You don't, you don't, you don't want your internal, a dedicated team to be doing software maintenance, you know, every week and then developing its own versions and force.

Right. So, so at layer one, I think there'll be consolidation over time. The question is, will. Because, you know, people are still, so does this negative aspect. Audience can feel free to disagree with me. There's this, uh, aspect of speculative investments that's driving creation of yet different, uh, blockchain networks, private networks for literally for the purpose of leery, you know, um, you know, what's the, what's the polite word say of saying this rising, increasing the price of the, you know, uh, endogenous token of that network.

Right? So it's self-serving right. And that can only last for a while. Right. You know, this particular network, so to [00:16:00] tokens has gone up price 30% this week. Why? Because some other company decided to use that service. Right. But then what happens? You know, if, if you repeat this multiple times, you know, we end up having a thousand different non interoperable systems.

Right. And there's no incentive to work together because right now the goal of many of these, you know, um, private asset net, which is to capture. As much of the audience as possible, so it's not in the interest to do interoperability.

[00:16:28] Eric: Right, right. I agree with that. So. Okay. So, so moving, uh, moving forward, uh, your, your paper, uh, actually it is a paper in draft, right?

The interoperability architecture for, uh, distributed ledger technology gateways. Um, so, uh, we'll include a link in the show notes. Um, but it is still a, it's still a work

in progress, but, uh, it's largely written, I guess, for collecting feedback. Uh, has there been a lot of feedback or you, you contemplate contemplating certain sections of it?

[00:16:57] Thomas: Uh, yeah. So, so a bit of [00:17:00] background about, about the it's called an internet draft. So in the IETF, the, the way, you know, standards are a form is through these drafts. And then if there's a sufficient interest, a working group is created andIETF waters, we went to the IETF is because it's an open organization.

So the idea is that, you know, what, what things can we standardize today in terms of writing specifications? And the reason is because if you look at the traditional banking and I think even future banking, um, there needs to be a written specifications. It's, it's not enough for some industry verticals to just have a.

User guide and say, well, that's, that's the RFC, that's the guide. Right. You know, so the, so that the IETF, um, uh, sort of spec process is very, um, you know, rigorous, right? So the, the drafts, you know, I've seen drafts some of the, you know, drafts like for the, uh, open, authentication token, [00:18:00] it went through like 32 different iterations.

So it's draft 0, 0 1 all the way to 0, 0 32. It took about two years, three years, very contained. And then it gets reviewed by everybody and then it gets reviewed by the security experts and then it gets, you know, so there's multiple cycles of reviews because often there's in precision in language that confuses people.

There's this other does errors, you know, literally. And that sometimes there are components. For example, if you're doing a draft on a particular cipher, a cryptographic algorithm, uh, you, you have to specify every byte every bit. And every function, you know, down to the detail there, there's no hand-waving here and it's, and it's a printed document.

And the goal is that if, if this document is to be given to an engineer that yeah, maybe you're familiar with the area, but it's never done it before that engineer needs to be able to integrate. I would say [00:19:00] 70%, 80% of the material in the RFC. And of course there's always going to be 20%, 20% percent of questions.

Like, what does this mean? What does that mean? Right. So this is, this is a normal engineering process and this is how you have interrupt because. You know, the, the, the documents that, that become RFC in the IATF, the authors have to surrender surrender. They have to give an IPR statement basically saying, okay, we are willing to give anybody maybe for example, ran non-discriminatory Tory sort of access to

our patents that are relevant to implement this draft because it benefits though industry.

This particular RFC of particular tech, you know, specification gets adopted because, you know, people want value and value typically lies at the higher levels of the stack, as you know, Eric. Um, you know, so for example, you know, in the, in the movie streaming industry, right, they don't care about the DCP IP packet, but it has to be there [00:20:00] everybody in the, in the network implement, you know, so the value goes up, you know, increasingly as you go up the stack.

And so, you know, um, there's a dependency then this is where this whole layer model becomes important. And I, I like the way people using layer one layer two is I think we're going to end up with at least layer four layers, L three and L four that's yet to be discovered, discussed, argued, you know, fought about

[00:20:27] Eric: for sure, for sure.

Well, well, humans have a way of, uh, making everything more complex over time with periods of consolidation. So, um, back to the, to the gateways, um, Let's define the gateway construct a little bit in terms of, you know, its connection points, obviously. So, so just to introduce the concept a little bit more, um, you know, there, you know, we've covered bridging before on, on the podcast, uh, we had a, uh, bridging [00:21:00] across 10,000 blockchains with Jack Lu and Weija Zhang of Wanchain

that was a, a great episode. We learned a lot about, uh, how bridging occurs gateways are different. It's a different methodology.. Right? And so that's what we're going to be talking today about it, which is that's something else being the gateway, but just from an architectural perspective, um, in terms of moving assets much in the way you do for bridging.

How would you, how would you describe, uh, gateways and how would you differentiate it from, from bridging just for the purposes of better understanding?

[00:21:34] Thomas: Sure, sure. So I actually listened to that podcast. That was, that was a very good podcast. I learned a lot, actually. So, so the, the idea of the, the bridge of the, sort of the gateway into IETF comes from the BG border gateway protocol, which is also a gateway.

And you can buy actual routers that expensive routers that implement the BGP protocol. So the idea of. The gateway [00:22:00] is that, uh, you have peers, so you have a one gateway that stands in front of one blockchain network, a one DLT network, and you have another one, a second one that, that, you know, stands in front of, you know, the, um, the second network.

And of course it needs to network. You can have multiple gateways and we can talk about how, you know, what, uh, strategies would you use to select, you know, a particular gateway and any point in time. Right. And, and so the idea would be that when you do an asset transfer right now in that yet we're just looking at unidirectional, right?

And, uh, if we, if we cannot do unidirectional, we wouldn't be able to use bi-directional or do all this fancy stuff like, you know, atomic hash locks so just something very simple that the IETF always fashioned them. Let's do the simplest thing and build from there. What's the findability. So here's the building block.

Uh, so you have gateway G1 in front of blockchain, V1. You have gateway G2 in front of blockchain B2 so G one is peered with G2. [00:23:00] So, uh, we need a separate mechanism for, uh, G one to discoverG2 that we can talk about that. So the idea would be that here's an asset that's in blockchain, B one, it needs to be disabled or extinguished.

So this is you you've heard this phrase before the, the burden, uh, what's the phrase, a burner or lock or, yeah, so you, you want to lock, uh, and eventually extinguish the asset, which has economic value, which is what makes it very complicated. And. Move the value, uh, to the second blockchain and recreate regenerate the value in the second block and assuming at the protocol and the packet, uh, at the L1 layer, this is possible, right?

It's, it's, it's quite conceivable. It's not possible. So for example, if I have a land certificate for, you know, by my nice, you know, a hundred acre property in The Bahamas, you know, in blockchain D one, and I want to move [00:24:00] it to blockchain, B2, and B two happens to be Bitcoin. Well, not there's packet in Compton, incompatibility, you can't do that.

Right. So, so assuming it's. To when you can do that. So we need a commitment protocol that is robust, and we've been looking at the traditional database commitment protocols, which is the two phase commit protocol. And actually it's the better one is a three-phase commit protocol. So the reason why we're looking at that, that particular protocol, because we want the traditional acid properties, ACI D, which is you want atomicity.

Uh, so, uh, while that unidirectional transfer is happening, uh, it, it can't be in defeated. It needs to be, uh, atomic done or not done. There's no, there's no half, half finished, you know, finish everything on, not, not finished at all. So this would be atomic, uh, see, it needs to leave both sides in the consensus state.

So consistency, uh, number three is, uh, isolation. So, so, uh, while this is happening, uh, [00:25:00] you know, you can't, you can't do double. Right. So, so this is, uh, and then, um, the durability, what it's done, it's done. There's no, there's no backing off. There's no rollback. Right? And so if you, if you made a mistake, you just send it back again, but, but you can't undo a particular.

Um, and so, so in distributed databases, this is the model that, that, um, has been used directly in high-speed transaction database systems. That in fact, underlying, if you go to wall street, look got all the networks and databases. This is the technology under the hood. They might not call it two phase commit or three phase commit, but, you know, um, that's, that's the paradigm that they use.

So we're using that between and G2. And so there is a number of issues. So in. Uh, you know, and we're trying to extract that some principle design principles, just the way the internet has designed principles. So, um, for block two, the first blockchain be one, you know, we don't know what that [00:26:00] particular consensus mechanism is going to be used in, in V1 or what packet data, data structure is going to be used there.

Does it allow locking? Does it support, uh, you know, escrow, we don't know, right? This is, this is the other problem that, that in order to be universal, uh, you know, we don't know how we cannot know in advance what B one is going to be. So the scope of work in the IETF is simply the, the facing side view on

Right. And the design principle is that a G2 does not need to know the interior constructions and designs and resources and addresses. And what have you of the other blockchain, B one and vice vice versa. Just the way today to routing domains. They don't need to know the subnets and sub-net IP addresses and the sub-net writing pro all of the other, you know, networks.

So you want to hide it. You want, I think, in, in the draft, [00:27:00] in the IETF draft, I think we said, um, opaqueness, what was the, the opaqueness principle? Right. So, so, and that is to promote scalability. The internet today scales beautifully because each network is opaque to other, it only shares minimum information about routes through the BGP.

Uh, routing product. That's the purpose of the BGP is to advertise that if you're on a rock to this particular domain in this side of the world, you can ride it through me. And that that's all, that's all it does. It says route available. Right? Right. So this is back the roots of BG. So this is what inspired the gateway to gateway protocol.

Uh, the second document that, that actually defines what this protocol is, it's called ODAP, which is a open digital asset, uh, protocol. And it's, it, it defines a number of

just relevant things like API endpoints, uh, what, where's the URL for the endpoint to talk to the API at, you know, gateway G one and G2 and [00:28:00] salt.

So all those details are being, um, defined in the second document called app ODP.

[00:28:07] Eric: And is, and would the gateway construction be dependent on ODAP? ODAP is, I mean again, well, maybe just to even take a step back on what ODAP is, it's sort of the, um, the standard, uh, th the standards for communication, you know, like I, you know, again, I come from Walsh, you know, from wall street, and I think in terms of like fix, you know, and fixes sort of like the, you know, you have your technical commercial side, but the fixed messaging structure is predetermined.

You can turn on and off different fields. Is that similar to

[00:28:38] Thomas: whatODAP that's exactly right. That's an excellent description. It's just defining some of the obvious and needed from an engineering perspective. Uh, constructs like API end points, identifiers. What does that, what by is that, you know, is it, is it my company.com/some something slash something?

Something, and, yeah. So in fact, in the group, um, [00:29:00] uh, w you know, we have a meeting every two weeks. Uh, that's, that's attended by quite a few people. We talk about profiles of ODAP. So if, if somebody wants to use certain fields, tick, tick the box, and certain fields to make, to implement, ODAP a particular instance, then we've been using, using the word profile.

So you could say, oh, I'm going to, I want to build, build a profile about app where one side is a traditional, you know, SWIFT backend network. And the other side is a blockchain. Great. But you know, you look at all that you still need to, you know, specify in gory detail. What are the, what are the, you know, um, choices of, of the fields that you're going to use in.

[00:29:44] Eric: So, so let me ask a different question. I do want to return back to ODAP, but we, we, we have some with the chop on, on the gateway to, so, um, but on, on the, on ODAP, uh, it, it is a standard. And so can the gateways [00:30:00] exist with other standards or is, is, is ODAP uniquely suited to those gateways? In other words, let's say the fixed protocol came in and said, this is, we love this gateway idea.

We're going to, we're going to create a fixed protocol for that. Or we're also gonna talk maybe a little bit about visa, which also seems like it's developing his own protocol and they say, Hmm, we love this gateway, uh, idea. So we're going to plug that. We're going to plug our, uh, protocol into that. Does, you know, so is, is, is, oh, more dependent on the gateway than the gateway is dependent on.

[00:30:31] Thomas: Uh, so, so the, so I think what we're, what we're trying to do in ODA is extract out those engineering details that will be needed anyway, so that you might call it this, we call it, we're calling it that, but if you, if you, if you transcribe it on a piece of paper and we do the same, it's just a new URL, end point it's, it's the, it's those very minimal, basic things that like, we need to, for example, today, if you are [00:31:00] developing a web service, right, then you define API end points, you know?

Well, you know, we, people don't argue, but his http anymore of about URL URI, it's a given because it's, it's, it's so, you know, minuscule, but, but necessary. And so I'm hoping. Um, personally, I'm hoping that the ODAP sort of gains popularity and we really invite people to come and to the IETF and participate in and tell us what's missing in ODAP.

Right. Because it's, again, it's still a draft it's it's, you know, um, it's still a long way. I believe personally, uh, you know, maybe another year or two, this knowing the IETF process, it there's that long. And, you know, uh, which is also good because I think good engineering takes time. Right. Um, let's do good engineering, uh, and take the time and do it right.

You know, uh, without having to go back and revisit because it's, you know, an audience may know we went through this profile with the wifi, but remember the [00:32:00] wifi security issue back in 2000, 2001. And that's because a lot of vendors jumped out and I won't name. Producing, you know, wifi, you know, to, you know, uh, was it eight oh two.one deadlift?

Um, a and the G why was it the, and the, and the cipher, the encryption algorithm was a week and people are breaking into people, other people's wifi, and then, you know, they can, they can invoke this special ITU police task group, TGI two, just to design the site. And then what happened was, uh, you know, there was this discussion, well, we'd have to replace the hardware.

We have to replace a farmer. And so it. Put sales of wifi devices on the stand sale for like two years, no one was selling wifi hardware. It's I feel the same thing, right. That if we rush too much and discover there's, you know, errors, you know, your, your private network that contains your assets, it might just become [00:33:00] unpopular unworkable, and you'd have to reinvest in, you know, fix your code and so on.

Right. And so that's why written standards, you know, is important because people need to read and think about this running code is, but don't get me wrong. IETF is about running code, right? So we love writing code. You know, Kerberos is all about go. I bet you could blame some of us that, that, that my T for, for going the opposite, we had the code first and then we had to ride the RFC,

[00:33:25] Eric: So, and so maybe what you're describing and I'll pull a page from something you're familiar with is like the way that we have like an ISO and an NIS T and even CMMC in the cybersecurity community, different standards for achieving it. And when you're actually, um, a lot of times, if you're trying to support a particular standard, I mean, this is the fields would be more definitional, but you'll do a reference to NIST and ISO and CMMC, you'll just connect all the two and nobody would say, oh geez, it's a shame.

We only have. We did that. [00:34:00] We have so many and not just one we've sort of operated in saying, okay, well this offers something different, a different nuance and ISOs with different certification standard. And over time, who knows, maybe it, maybe it coalesces, or maybe it doesn't, but it's not really that critical that there'd be a single standard.

I mean, now you have another standard coming along and it just evolves and it doesn't mean you like say, okay, we're immediately shredding the other one and starting with the new one. So in many ways, like, you know, to the extent that doc, the, the ODAP is, is evolutionary, um, yeah, it could be different standards.

It sounds like what you're basically saying is there could be multiple standards. You might need to map the standards, like, right. If you say, oh, well, we did our standard on DAP and you did yours on the visa standard and like, oh, well, Which fields are, which, and just sort of map it, but then once you've done that mapping exercise, you have two different standards or three different, but you've mapped them.

So that's

[00:34:51] Thomas: right. That's right. Exactly. Right. So, so there will be multiple standards for the multiple components. So for example, talk about bridges and, uh, and the [00:35:00] UPC hub, right? The universal payment hub. I mean, it's conceivable that's, you know, we, we've spoken to the visa guys before and they've, they're very aware of the work in IETF and, but it's quite possible that you use theIETF gateway construct between your network and the UPC hub on one side for the bridges that the one Chan was talking about, you could do the same thing.

Right. And I think, and that's only, you know, the, the, the two phase commit that's implemented by ODAP. That's only a small slice, or it needs to be implemented. There's these other issues. And that, that I, I think I alluded to maybe, um, it'd be in the draft, this regulatory and jurisdictional layers, right?

This is, uh, this is, uh, this is what makes it complicated. So in, in the, in the, it, in the internet architecture of what you're trying to move is a set of. And packets and, and the send under receiver maintain the contextual information at the edges. And this is

called, this is a famous principle. It's called the end to end [00:36:00] principle that we take for granted today as being like blah, obvious.

It wasn't, people had huge fights in the late eighties about this, because there are people who were saying things like, well, we need to put the packet encryption inside the network, right? As part of the core network of the, of the internet. And people say, well, if that's the case, that means the network needs to be aware of context in this case, the security associations between the end points and the, and the keying material, which makes the whole internet design very, very complicated.

Right? And so the luckily the correct guys won the day. We said, no, no, no keys encryption. That's outside the internet design. I hear it. You know, people today complain about the internet is broken because it doesn't have identity. It doesn't have, it was designed. It wasn't broken. It was designed that way so that it could scale.

It was intended that you're supposed to build your identity layer on top of it. And I think people have beginning to realize that we kind of need the same thing. If we want to have the internet of [00:37:00] value for assets and blockchains, you can't cram in everything into one layer. You need to, you need to figure out your layer architecture up and down and say which section goes where.

And so one of those layers is going to be, uh, you know, AML. This is I've been calling it, the AML layer. This is, this is the stuff about, um, tracking, which entity holds the particular assets in an, and so who's the, or in, in, in terms of an asset movement across gateways, across networks, who is the originator, who is the beneficiary, this is the.

Right. And then the FATF model F a T F is the help me, Eric. It's not it's

[00:37:42] Eric: the financial action

[00:37:45] Thomas: taskforce group. It's the people who deal with the problem. AML have been dealing with anti money laundering and so on for like, what is it? 25 years I think. Yeah.

[00:37:55] Eric: Yeah. There's like a, it was 190 countries or something and represented.

And [00:38:00] they, there, they have status offer guidance and standards and the jurisdictions have to adopt them. And they blacklist jurisdiction.

[00:38:08] Thomas: No, no, no. The advantage the gateway in its, in its very basic form gateway to gateway. It's this old app and you could use it for a bridge. You can use it for an UPC hub connection.

You can use it for many things, but when you begin addressing specific use cases, then certain other layers have to come into. So one of them would be this AML layer. So, um, question then becomes, so if, if, if, if I want, if I was a network here, I had an, I had a gateway and Eric you're a net network in The Bahamas and it has a gateway and I want to move assets to your account in your network, through these two gateways.

Do you want to, and G2 the problem becomes well before you do that, uh, are you complying to local AML regulations in both countries? Right. And the, the sort of the minimal, [00:39:00] um, very minimal, I would say sort of agreement is, is defined in the FATF recommendation, 15 and 16. And, and I believe there's a few updates, you know, I think there's a recent update there, and that is that, um, before, or at the same time as the asset transferal, you have to also transfer information about the individuals, the originator, but me and you be, you know, that's doing this transaction.

Right, right now, the question becomes. In this particular use case who is operating the gateways. If the guy does have, how to gateway is implementable. It's a single server with, you know, expensive hardware as on song w where they it's in a VM up in Amazon. AWS does it doesn't matter who is responsible legally for operating that gateway.

And this is called the VASP virtual asset service provider in FATF language. If you know the VSP kind of, you know, kind of paint to say VASP. Uh, but, but, so the [00:40:00] question then becomes when these two gateways begin to open connection, you know, then eventually, you know, implement, execute ODAP before they even get to the ODAP stage, they need to find out who these guys are.

So. I'm a gateway here in Boston. Uh, I'm owned by this VASP, you know, number one and in the gateway, in The Bahamas where your network is, where your asset is, it's owned by, you know, VASP amount, number two, who either who had these companies that they illegally registered, do you have, do they have an LEI number, right?

And this is where this whole discussion about, well, how can we automate automate this so that when do you want, wants to talk to G2? He already knows within a split second, that they're both legitimate, um, registered businesses who own and operated. Uh, it could even if you want it to, um, inquire about the technology that

implements the gateway does, this is about gateway attestations, which is another thread that, that is being discussed in the IETF.

Um, and then once they do that, they can [00:41:00] open, you know, a secure channel, you know, we're not defining word is you were just saying, TLS is kind of your base secure channel. And then you can start talking about, you know, implementingODAP and, you know, two phase commit or three phase commit, right? So, so there's these layers things need to happen first at, I think, uh, at, at the legal layer before we can actually move assets.

And the reason is because when you moving assets, unlike the internet, it's not just moving bites, you're moving economic value right in and out of network. And that can have indirect impact on the bigger economy, uh, on mainstream economy, as, as the economists, you know, will tell you this there's many reports that talk about this, um, problem that, you know, crypto is not the script.

It's not just by it's actual, you know, you know, economic.

[00:41:48] Eric: Right. Right. So, so, and just to kind of circle back, excuse me, to, um, that core distinction with bridging. Um, so, [00:42:00] so in a bridging context, typically, you know, I, I don't, you know, I often think of bridging is something you do to convert your asset to something else.

And so that you put in something and you get a wrapped asset back, and then you can transact. Um, but I suppose in terms, if you're doing trait Paris and what have you, you can do it instantaneously through a bridge, it's a similar process.

[00:42:24] Thomas: it compliments. So I look at bridging as the next layer up.

So if, if you have, you know, an entity or, you know, providing bridge services, in fact could implement the gateway function within its. Right, because, because the word bridging here, there's a connotation because it's, it's not just moving. Uh, you're you're converting. So, so let's say blockchain B one was currency one and blockchain.

B two is currency to somebody who's running a bridging network would say we have our own temporary, local token or currency, you know, call it currency three. And what we do [00:43:00] is go from one to three and three to two, and so great. That's one solution you could pursue, but underneath there, you still need these two phase.

You need commitment, right? When, when you move this inside in the bowels of your network, you will need those four properties at ACI D properties for your own security, right? Because if suddenly your network gets hacked and, um, your, your conversions are interrupted, right? So in fact, you could even say, well, maybe this two cases of.

Um, commitment that's needed. So from they see what the car is, C3 that has to happen atomically, and then from C3 down to C C to the second doctor. So yeah, to me, this is a great compliment that in fact, the whole bridging concept is a richer, uh, sort of construct that wraps around the gateways. Then in fact, one of more gateways will be needed that implements this ODAP commitment, [00:44:00] uh, you sort of unit unidirectional, right?

So you could have, you know, you can implement a bridge that is bi-directional right. It's this, it's this more of the same staff, the little units inside the ODAP

[00:44:12] Eric: instantiations. Yes. So, so it's interesting when I was reading the paper, it occurred to me that it, you still, you know, you're, you know, you could potentially over time remove some of the third-party intermediation.

But you're still going to have to have certain components maintained by third parties, irrespective like security layer, you know, or

[00:44:36] Thomas: yeah. And it could be, it could be that in the future, there will be many of these bridging networks and that your gate is solid. If you are a private network, you know, you're a consortium of, of enterprises.

Your gateway could have an additional function that just cancer, the cost of conversion, just like, did they arrive when you buy, you buy and sell us dollars? Right. Do you know which, which [00:45:00] particular exchange service bridging service gives you the best value today? Right. So could, could you automatically choose, okay, I'm going to send, you know, a hundred million dollars to Eric and The Bahamas.

I could, I could use, you know, something like, you know,Wanchain today, you know, maybe somebody else tomorrow, why? Well, because somethings the price of the, uh, you know, conversion fee has slightly gone up. Right. And that needs to be automated. Then in the future, these, these transfer gate. Pick the cheapest route.

Just, just the way, just the way the internet today, when it picks, you know, routing, it picks the best ride and the best is, is not the, the perfect it's the, uh, what's the, what's the phrase there, the, um, uh, best, uh, uh, best grade, what's the phrase I'm blacking out. It's, it's, it's the most optimal rod for this particular context.

Right? So it could [00:46:00] be the same thing, right? Uh, so I'm going to ride by this particular bridge or that bridge because it's optimal, you know, the fees the better for me today. If I use bridge bridge, number two of bridge.

[00:46:13] Eric: Right. And I also suppose that this kind of construct, like let's just take swift, for example, where you have a network has to be enterprise grade.

Maybe they don't want to rely on public, you know, public blockchain type resources. They effectively want to build maybe a, more of a closed network, a membership-based network. Um, presumably they could use this as a building block to facilitate that, that kind of a fully enclosed system. Right. And

[00:46:41] Thomas: that's right, exactly.

Right. So, so the, in the draft we even say, well, you know, so there's two principle, right? So the principle, the first one is opaqueness, you know, uh, uh, principal. Uh, and second one was, is that ODAP needs to be oblivious to the economic value at the ODAP layer. Is this. [00:47:00] That's it, it doesn't, it doesn't know anything.

It's it shouldn't know anything about the economic value that's that's at the bridge layer or, or some of the layer above it. Right. So, um, in the, in the, in the case of, of, you know, something like, you know, uh, you would like to be able to have one side, literally be a traditional banking, maybe it's swift on one side.

Right. And the other side it's any number of available blockchains today. And so when an engineer in this, you know, surf engineer sits down and says, oh, how do we do this? These, this is the where the ODAP choices, as you said, like which, which options fields that we're going to use in ODAP for this particular scenario, because one side we've got these banking network and it doesn't know anything about.

He doesn't know what a hash block is. It doesn't know what a Timelock is. It doesn't know all this fancy stuff. In fact, it doesn't even probably use, you know, um, elliptic curve, cryptography. It's probably still using [00:48:00] RSA, you know, so that's one site and then just, and then the engineer has to go that. I said, okay, well, you know, who are we talking on the, on the blockchain side, on that's under, on the second side.

Well, you know, maybe it's the Ethereum great. Well, we have these tools available when we talk that you theorem, but then you say, well, actually it's, instead of a theory, maybe it's an instance of fabric where it's got a different construct yet. Right. And so, so the, the, the, the Harmon sort of context in this, you know, in this, uh, gateway is this ODAP , but it's ODAP on its own is insufficient.

You need all this other stuff that addresses the particular connection scenario or using.

[00:48:41] Eric: Right. Right. And, and so now, just to get back to, um, the, the FATF point that you were talking about, do you see, I mean, for that reason for, you know, for what I described, like a swift network or some other, uh, financial intermediary or VASP type network, do you, do you see that, [00:49:00] that this particular construct is going to be more appealing?

W you know, in terms of AML compliance then than possibly other networks where maybe, you know, it, that the AML compliance is, you know, it's a third-party protocol or something, but you're talking about like enterprise grade level such as is that, does that where you see probably the primary use case.

[00:49:25] Thomas: So, so the question of, of, um, so these are so AML, AML, the travel rule, it's all about data.

Person did individual data originated in a beneficiary data and of course, VASP data, uh, you know, business data. Right? And so, in a sense, it's, it's disconnected as a separate layer. It's probably two layers up from, uh, this, um, the, what I call the gateway, you know, layer. And so the challenge in the FATF a situation is that, uh, uh, both sides VASPs now have the [00:50:00] responsibility of making sure that the originator data, personal data is accurate.

And, um, the same on the, on the beneficiary side. And the problem is that, um, these VASP need to actually send personal data. So if, if I was going to send you, you know, you know, assets in The Bahamas, Eric, my VASP in Boston actually we'll have to set sent to your VASP in The Bahamas. My first name, last name, address, account number here in the Boston.

Uh, I think probably email address. Right. So, so that's great. But I don't know, as an individual, as a citizen, I don't know what data privacy regimes or regulations are being implemented in The Bahamas by the VASSP because the last thing I want is my personal data to be sold off to data aggregators, that's quite common and vice versa.

Right. And so there's this problem. And, and so, [00:51:00] uh, we gave a presentation at FATF in 2019 in the Vienna meeting just before recommendation 15 was, was produced. And we kind of suggested that, you know, maybe these VASPs need to get together and form their own network. Uh, that's offchain that has nothing to do with blockchains, you know, directly for the purpose of exchanging, uh, customer personal data securely, uh, and observing some common, maybe global private data, privacy rules segment, as such as the.

Right. So that, so a VASP as a, as a business, it needs to be a registered, of course it needs an LEI number. And then when he joins it net this network, it needs to sign a contract and a membership agreement saying that if I receive personal data from people. You know, you know, in belonging to B people are customers of other VASPs in that community.

I promise not to be leaking that out and, and [00:52:00] selling it to the marketing companies. Right. Um, because you know, you, you know, Eric, I, you know, if I send

you, you know, uh, you know, a hundred million dollars, you know, today next, next, next, next day, I'll get all these junk emails from, you know, a luxury car manufacturers trying to sell me cars.

Right? Like how do they know? Right. So this is so, so, so, so that's one side, and of course, this is all about anti money laundering, right? And so that network needs to be visible to the government so that the government can enforce whatever AML regulations they need to enforce. Right? So people talk about, well, let's use zero knowledge proofs for this, you know, personal data networks amongst of us.

That's great, you know, use whatever you want for data privacy and privacy preservation. But don't forget that the government is in there as a part of. And they need the capability to figure out, you know, entities who are buying and selling or, you know, sending assets for the, for the purpose of anti-money laundering regulations.

[00:52:59] Eric: [00:53:00] Right. And I suppose there could be a way even, I think one of the things that's talked about is like, how do we get to the least used, uh, you know, a scenario where you don't provide access to, to. Then you absolutely need to. And I think maybe that's where like Z KP or, or, you know, I suppose you can even design it as a fully homomorphic encrypted, uh, network.

Um, although, you know, it could be SMPC, you know, there's all these, you know, homomorphic encryption as a way to go, uh, you know, in terms of scalability, but, um, you know, whereby the, the individual ASPs may not need to collect all that data. They just may need to know that that data has been collected by a credible source and, and, you know, and that it exists.

And then presumably the government authority. Where somebody else could also access it if they needed to, but just to limit, you know, because in a lot of cases on the regulatory side, you know, regulators are used to collecting just reams of [00:54:00] data, you know, enormous amounts of data and, and, you know, sharing it with all these different algorithms and et cetera to conduct surveillance.

But ultimately, you know, to the extent that those, that, that information is available or represents a honeypot, then, you know, then, then great, you know, the regulators have it, but the bad news is that, you know, any individual regulator might be just insecure, you know, and, and you know, all you need to do is figure out which one is the weak one and you get all that data.

Whereas if it's like, you know, I, I often think in terms of like a red flag, like if something's flagged then okay, then that's the basis upon which you, you collect the data, but in the absence of a red flag, You know, you're, you're, you're conducting

your testing and everything else in a fully encrypted fashion and not, not necessarily revealing it or subjecting that is all new

[00:54:48] Thomas: abilities.

That's right. So this is another frontier exciting frontier. So our connection to science is, um, helping with a group called TRISA travel rule information, sharing [00:55:00] Alliance, if you people just TRSA. And you'll see the website said that the goal of TRISA is in fact to look at this new infrastructure to support the sharing of this personal information among vests, right?

So it's open to any and all kinds of privacy, preserving, uh, technologies. And we've had presentations and people thought about zero knowledge proofs that people talking about just straight encryption. But, but I think, uh, right now the. VASP community exchanges. They need to realize that they need to get together and form this data network data exchange network on their own and, and, you know, provide some, maybe even standards there, uh, so that, you know, like which fields are going to be sent, you know, and you can even, you know, grade, you know, end points countries, you know, oh, well, you know, this asset is going to be a customer has asked for a thousand dollars to be sent to this remote, you [00:56:00] know, you know, um, country over there and some other continent.

Um, and we don't think it's secure enough. So we're going to tell the customer, you know, what if, if we sell this, send this thousand dollars, which is permitted under, you know, under sec regulations, we still have to send your personal data. Are you willing to go ahead? Right. So, so the customer, the individuals need to, uh, be aided health.

By the tools and understanding that, you know, sending crypto is not to sending crypto there's other. Implications such as well, possibly your persona data could be also sent through this remote place. And after it skip, it gets there. We don't know what's going to happen. Right. So, so, so that's an exciting, um, also, um, frontier, uh, and I invited folks to look at, you know, TRISA that, you know, and this is, this is, you know, part of a bigger, um, dialogue with some of the big, um, exchange networks.

[00:56:55] Eric: Um, one of the things I noticed in the paper, it talked about the [00:57:00] importance of, of, of log data in terms of verification. Um, you know, and that's, that was interesting to me only because I, you know, when you think in terms of bridging and such, you're thinking, you know, you're basically looking to the blockchain, the immutable blockchain for a lot of these things, which is not to say that you wouldn't also review the logs.

Do you feel that the, that, you know, collecting and retaining and analyzing the logs. Is of greater importance in this kind of network.

[00:57:28] Thomas: Sure. So, so in the, um, gateway drafted a document, um, this, this question of crash recovery, right?

So, so, uh, if you, if you have, do you want in G2 are communicating, uh, today's practices in, in database, you know, um, consistency of management between the super database, uh, transaction oriented, you know, protocols, uh, the, the gateways, the databases, uh, retain local logs. And the reason is that if the machine [00:58:00] dies or crashes, it doesn't have to re.

Uh, the session from the beginning, again, it can just say, look at its own local law. Presumably it's on disc, presumably there's a disc that survives the crash boot shop reads it like, oh, I'm, you know, out of the 11 steps, I was up to step five. And so I don't have to repeat step one before I can resume the previous session.

So that's in the, in the ODAP case, uh, when we say log, we mean crash recovery log locally, and then we've talked about, well, should we, should we record the log inside? You know, a blockchain or DLT? Yes we could. But what, you know, what does it give us? Because. For fast, you know, reboot and recover in session resumption, you need the laws to be available either in memory or on disk, worst cases on disc.

[00:58:48] Eric: Right. So, so, so it sounds like the log, uh, the like retention is probably really no different than like, uh, the way that a node operator would retain logs similarly. [00:59:00] Okay. So, and, and you wouldn't, you know, and, and so you wouldn't place any lesser or greater importance by virtue of the fact that you're using a gateway versus using a sort of a public bridging network.

[00:59:12] Thomas: Huh? I think the gateway is, is the protocol that implements the bridging, right? The bridging is a higher layer layer concept because it includes this notion of value. And that's this notion of economic value is outside the scope of dieting where we said, you know, I've got a bunch of slides to say, okay.

And in fact, the principles about opaqueness and, you know, this end-to-end context says, well, The two gateways are not aware of any currency, any value whatsoever. Right? So, uh, I think it's a great compliment to bridging and, you know, we're looking at the idea, well, if you have a bridge and to end, how many gateway pairs do you need [01:00:00] under, uh, in the hood?

And I don't need the hood inside, inside your, your bowels of your, of your bridge network. And it looks like from the outside a good bridge looks like a simple, straight uniform connection. Right. But underneath you said, well, okay, maybe

there's, you know, two pairs of three pairs of gateways. And that's where kind of there at the, at the minuscule sort of layer there just, just between two gateways.

[01:00:25] Eric: The gateway is a way of, is, is a way of facilitating the bridging a way of standardizing the bridging. But it's not like in lieu of

[01:00:35] Thomas: no, no, it's not.

[01:00:35] Eric:

[01:00:35] Thomas: I, I do hope that the bridging community sort of begins to look at the need to standardize the end point.

Right. And, and the actual bites going across the bridges. Right. Sorry. And if there's a third currency involved, you know, w you know, that's mediating the exchange. Well, then, you know, you need to also define the bytes that, that reference that currency.

[01:00:59] Eric: [01:01:00] Great. Great. And do you see, um, what gateways there being any sort of limitations in terms of, uh, you know, cryptography, like I

[01:01:09] Thomas: there's, uh, new technologies such as using T E secure enclaves, you know, things like SGX.

Uh, we're also very involved in the CCC, the confidential computing, uh, consortium, which is an Alliance of people who are using some of this T E uh, technology to create the future secure, competent, secure computation environment. Right. And that, that has a lot of challenges, but it's a great set of, you know, we've looked at well, you know, could it be used to ease, to implement gateways?

Right. That's right. Why not? You know, I, in my gateway here and your gateway in The Bahamas, we could all implement TES and then it, it, you know, it could talk to each other using that kind of trusted hardware or so this is another exciting frontier, at least for me, [01:02:00] as I said, this is a, you know, I hope the audience appreciates that we're living in very exciting times and rugby, uh, this is, this is the next, this is truly the next sort of iteration of the internet.

[01:02:14] Eric: Yeah. And I think even more exciting. But, um, so, so, so then in that context, we mentioned a couple of different, uh, you know, forms of cryptology and frameworks. So w so obviously T E would be on the top of the list, which other ones do you think would, would be well-suited and you don't have to, I won't hold you to this answer forever.

You know, if it changes in six months, it'd be like, well, that was six months ago. So your.

[01:02:43] Thomas: So, so that's an interesting question, because I think as an industry, as a whole, and I'm talking about the, the, the big players that, you know, who, who, particularly people who provide cloud services. So for cloud providers T is offer an interesting technology because now they can [01:03:00] create farms of servers, uh, where your server hardware supports the ease.

And, uh, as a, as a, as a sort of grid of these D E bosses, you can essentially expose, uh, you know, trusted computing space to the end-user the customer. Right? And so, um, it's, it's early days. And I think you've seen probably out there in the market, maybe Intel SGX to whatever the version is now to point something it's kind of.

Most popular, um, from early, because I think it comes with the high end Intel processors, right? You don't have to buy any special processor, but, and this several competitions is, you know, out there arms got a solution and B has got a solution. Uh, I think for the industry as a whole, uh, they will need to standardize on certain aspects of proving, uh, testing.

That your [01:04:00] hardware is a true T so because if, if you are, so here's a good example. So if I was, if I was a biomedical service provider and I have, you know, very sensitive data as CA cancer data for, you know, the, the politicians in Washington, DC, right? Psycho who's got cancer. This is, this is very, very, you know.

And so I would like to be able to compute or do data manipulation in a trustworthy space, but before I load my data into your cloud, the claims. This technology you need clap, provide a, you need to be able to give an attestation back to me about the construction, literally the composition of your stack from hardware firmware, all the way up to the, uh, VMs, uh, and the, um, containers that are going to be running inside this execution environment.

So we're at the cusp of, of [01:05:00] a fairly complex. Um, technology out there, right? It's, it's one thing to say something about the tech, you know, your infrastructure. It's another thing to be able to prove it sufficiently. Right. Right. And this is another ad we've been active with tricep computing group for like 20 something years, not 21 years.

Uh, and the ICF, uh, of all places act two also has a group called, uh, working group called rats, remote attestation working group. That's pretty much the same bunch of guys from the TCG, but it's IETF. So it's an open process. Uh, I invite people to, to, uh, read that. In fact, the just last week, the group just voted the rat's architecture to be an RFC proper.

So it's going to be, uh, and the second year and a half, two years to get through this agreement on this architecture only because it is fairly complex. And I think there's a

lot of synergy between. RAs [01:06:00] architecture, TCG, you know, secure computing architecture with the whole crypto space, because we see that in the future, it could be that crypto transactions need to be made private.

Right. But you need a way to prove safe to the government that yes, this transaction occurred in this infrastructure at this particular point in time. Here's a copy of it at the station that they received from the infrastructure provider cloud provider. And here's my side of the evidence that I loaded up, you know, my side of the transaction to that particular T and vice versa.

Right. So again, fairly, fairly complex, fairly interesting and exciting. Right.

[01:06:42] Eric: So, so, and, and just to kinda summarize this as I understand it, you know, Presumably any type of encrypted framework, whether it's homomorphic or secure multi-party may make sense in sort of a non standardized wider adoption context, a smaller [01:07:00] closed network, you could do whatever.

Right. Uh, but, but if you're thinking in terms of how do we do something, that's going to be more universal. That's going to be more widely adopted. Tee would be, you know, sort of where you'd go first with remote attestations, as opposed to, I mean, homomorphic encryption, it has to be, it all has to be largely closed.

[01:07:17] Thomas: And in fact, this is another role for the gateway is that imagine, you know, blockchain be one, all the nodes there, you know, there's a thousand nodes, you know, doing consensus and implementing some T mechanism in hardware. So you can see, you know, people from outside, can't see the, the ledger, the ledger is always perpetually encrypted, but you want to move assets out of that network.

Right? So, so this gateway needs to be. Looking in, it needs to participate in this whole private computing space that it can know that there's no double know same rules, no double spending members can't cheat, all that stuff. So it needs to be able to peer into that encrypted space. And then at the same time, [01:08:00] be able to talk to the outside world and move assets across again, with the same acid acid properties, the atomicity properties, right?

And this is, this is why the more we look at it, the more we sort of think, well, you know, this gateway construct is sort of the, the smallest unit. It's, it's literally the, you know, right at a Ryder connection about which you can build all sorts of fun stuff, but it needs to have this unit down there. So this is great, you know, great aspect of this gateway is this whole.

You know, private blockchain and crypto blockchain, sort of, you know, uh, I, I think it's an upcoming area that's being studied by a lot of people.

[01:08:42] Eric: Right, right. Well, it's interesting. Cause I mean, it really sort of, you know, I think it's helpful to look at the gateways as sort of functioning within both in sort of a larger, broader, universal context, as well as even an integration with, with individual private networks that might have different crypto crypto graphic properties.

[01:08:58] Eric: looking at the, the, [01:09:00] the visa, uh, universal payment channel hub under development, um, could you offer some money? Um, I don't know if you've, I'm sure you've read the paper. You said you spoke to them. What are your thoughts on that and how it, how would you compare and contrast it with some of the work that, that you've been working on?

[01:09:20] Thomas: Like the bridging concept. This is a great compliment. So, so, uh, my understanding of the, of the hub model is that in fact it is going to be an, a hub. You know, model and the, and the hub could be something that visa could run as a service. Right. And so we see, you know, let's say you have blockchain, be one that needs to talk to blockchain, be to via this hub.

Well, between each of the blockchain and the. You would run a gateway protocol such as ODA app. Right? So underneath of course, there's all the bells and whistles and all the features to non-relevant, uh, meaningful to the hub, uh, and on a, on a [01:10:00] business sort of strategy. I think that's a very smart strategy on the part of visa, because getting the, you know, right now the card payments industry is the industry that interfaces to the end user.

Right? Most of us, particularly in developing countries would be using some kind of a card. And of course, there's now on your, on your phone, do you have NFCS and so on? Um, uh, near-field communications, um, you know, chips that allow, you know, your credit card to be stored, right? You can just shop using your phone.

Right? So, so, um, for entities who are particularly visa, MasterCard, and so on, who are running card payment rails, Essentially the challenges, what would be their role in the future in this whole sort of, um, decentralized digital currency space? Can they repurpose their rails because they haven't built the rails?

What I mean by rails is the, the network that communicates transaction data [01:11:00] from the issue, the point of service terminal, uh, up to the, uh, uh, merchant bank all the way to the issuing bank. So there's this parallel network, you know, that, that in fact, just this delivers transaction data, you know, Thomas went to, you know, stop and shop or, you know, seven 11 and, you know, spend $20.

Well, that, that gets the ride all the way to my issuing bank. Let's say I was a member of, you know, card member, cardholder of bank of America issued cards. So that

network already exists. So the question for these people, uh, this consortium of companies who own and operate this. What I essentially is a data network.

How could they leverage that into this new world of digital currency and tokens and stable coins? And I think the hub model makes sense for people in that space as, as a possible future model. Because because today they are a kind of a hub and spoke, right? The, the merchants, uh, online and the [01:12:00] real world, you know, they're part of service terminal.

They talk to a, to a hub already. So it's, it's this, it's this a transferal of the same hub and spoke model, but into the blockchain.

[01:12:13] Eric: Right. Um, and I suppose that, that even the adoption is such a hub and spoke model. The UPC is probably a bit of a threat to the, to the banking

[01:12:21] Thomas: Yeah. It's so, so we, we like the sound that we've, I've said it several times publicly.

I mean, banks are in the business of trust, right? That's what they do. I mean, yeah, there happened to be holding this bits and pieces by and bits. That's called money that I access through my, you know, ATM card and my Tim card can produce pieces of paper. That's called, you know, money, but the majority of my transactions are card.

Right. So, so, but I trust that brand. And I think the role for banks in this space is in fact to provide trustworthy services, regardless of how [01:13:00] the assets or currencies are transferred, whether it's point to point, you know, maybe it's using some kind of a surf is a payment rails, or maybe it's a blockchain, right?

So it's, it's conceivable that you could replace the surf network with an advanced sort of blockchain based network that does the same thing. Plus, plus. Other stuff. Right, right. That instead of just sending transaction data, maybe it could also be running its own settlement coin, local coin or token. So to all the baskets settled very quickly.

So that, so that the people who are familiar with the four corners model of the card payments that the merchant bank and the issuing bank could sell literally in seconds versus having to wait overnight, I think, which is what happens today. Right? So there's a lot of improvements in speed. And at the same time, I mean, the goal is really to reduce costs to the merchants and to the consumers.

Right. So, so I think, [01:14:00] I think no banks are going to be around, I think a long time. It's just that they might be doing things different than what they do, you know, traditionally

[01:14:09] Eric: for sure, for sure. Do you think, um, like what do you think are some of the biggest challenges to whether it's the UPC model or the gateway model?

Like, do you believe that scalability, like the standardization, obviously it facilitates scalability, but where do you see the choke points? Uh, you know, along the road?

[01:14:32] Thomas: Hm trade-offs yeah. So, so definitely it's scalability of, of service. Um, another one that's gets rarely discussed is, um, what is the value to the main street economy?

So, so, so the CBDC discussion, particularly for commercial banks. So for the wholesale CBDC space, okay. You can, you can improve, you know, the speeds and optimize and so on because it's all commercial banks, right. [01:15:00] And it might provide them with, you know, gains, but for main, for retail, CBDC, you know, um, from, you know, mom and pop people like you and me.

There's this technology provide advantages over the cot payments infrastructure. So the needs, you know, if there's no advantage to the end-user and there's no, uh, improvement in the user interaction and user behavior using payments. If I S if I still go through stop and shop or 70 11 and swipe my phone, you know, on top of the pasta terminal, well, there's no change for me.

I mean, in fact, I, it's almost like I'm oblivious to whatever happens in the, in the back. Right. What I do care is, is as a consumer, is that, well, you know, uh, my, you know, APR percentage, you know, penalties for late payments is lower if I use this new kind of technology. Right. So things like that matter. So that that's the second [01:16:00] challenge.

And I think. Yeah, probably thirdly, is this, um, separation of standardization from, you know, incentivization. So, so let me, let me, this is an earlier point. I mentioned that that, um, a lot of speakers, you know, investors are, um, you know, jumping on this technology just for speculative investment, which is great.

Right. But then at the same time, I think, and not enough resources financing and so on are being directed at standardization, which benefits everyone. So again, back in the internet days, um, DARPA, you know, funded the start of the internet, you know, in today's money is several hundreds of millions of dollars.

Right. Um, and, but then they have a particular bad, a particular threat in those days, the world had a threat and that was the cold war and that was driving it. Today, we don't really have a threat other than certain big nations in the Asia [01:17:00] Pacific region, you know, challenging the dominance of the us dollar.

Okay. So as a, so that, that could be perceived as a threat that warrants, all this investment is in this new technology, but I haven't seen that urgency. Right. Right. People are like, ah, you know, in fact, we, in certain communities, but your engineering communities, there's almost a cynical view on, on crypto and blockchains and so on because they all say, well, it's, you know, so far it's just speculation and there's no imminent danger of the world collapsing that we have to like pay attention to this technology.

[01:17:35] Eric: Right. Right. Well, I think in the CBDC front, but yeah, the U S tends to, um, move a lot slower, more slowly, uh, because of the democratic process and also the political politicization of it. So. Well, great. This has been a great discussion. I feel like we could go on. Um, but, uh, thank you so much for coming on the podcast.

It was excellent to [01:18:00] have you and hear your insight and we'll include the sites of the papers in the show notes as well.

[01:18:06] Thomas: Thank you so much, Eric. Yes, we could talk all day. This is getting exciting time. I'll have the listeners audience and home realize yes. You know, get involved, you know, read stuff because this is going to impact your children, your grandchildren.

So, you know, and again, technologically for me, this is an awesome time to be, you know, to be alive.

[01:18:25] Eric: Yeah. Same here. Same here. Well, thank you so much.