Deloitte.

Legal on Air – Der Steuerrecht Podcast von Deloitte
Episode #23: „Krypto verstehen – Folge 10: Zodia Custody“
Speaker: Alireza Siadat, Azmina Keshani

Alireza Siadat: This is a new episode of “Krypto verstehen”, or as we say it in English, “Understanding Crypto”. And today I'm very pleased to have a guest who's explaining to us what crypto custody means. We have Azmina with us from Zodia Custody. Azmina, please go ahead, introduce yourself and also what Zodia Custody is doing.

Azmina Keshani: Hi, Alireza. So thanks very much for having me on your podcast. It's a real honor to be here and to speak directly to your listeners. A little bit about Zodia Custody. So we are a crypto custodian originated out of Standard Chartered Ventures. As you know, we are operating a regulated custody business in eight jurisdictions globally. And we also have another product. So we have Zodia Solutions, which is where we provide infrastructure in relation to custody as a service. So those are the two main services that we provide. And our head office is based out of the UK. Myself, I'm a crypto lawyer. I started my life off as a custody lawyer and grew into crypto. And now as a general counsel of a crypto firm covering many topics, not just crypto regulatory, but also, you know, vending machine contracts. You know, all the bits and pieces that go around that.

Alireza Siadat: That's quite exciting. I think our listeners, they have a good understanding what crypto custody is and maybe also good understanding of Zodia. But let's start putting it in the right frame. So today we're going to speak about crypto custody under the markets and crypto assets regime. For those who are not familiar with it, which is the crypto assets regulation within the European Economic Area, which covers for the past 18 months and also for stablecoin issuers, I think for the past two years, the crypto custody regulation. And the grandfathering period is going to end soon, or maybe now you're going to listen it and it already has ended because this recording is right now live, but you will listen to it a little bit later. So I want to talk with you about what you believe. How do you see the European crypto assets market under the MiCAR regime? And to give like a better picture, we have roughly 200 CASPs. Many of them are in Germany, some of them are in Netherlands, but also some of them are in Luxembourg. And you also have a good relationship with the Luxembourg market. So maybe also from that perspective. So how do you see that?

Azmina Keshani: Yeah, so I would say the MiCAR process has been rather exciting and maybe a race to the finish for a lot of people because the transition period, as you know, was different in different markets. So a lot of providers have been very challenged in how they make sure they maintain their business and keeping compliant and while racing towards the finish line and also working with the regulators. You know, the regulators are learning this subject and we are working with them to educate them and support them because, you know, everybody wants the same answer. We want to build this market. We want to be a leader in Europe as well. So I have to say, you know, I've been very impressed with the CSSF in Luxembourg. They have been a great partner to us and worked very closely with us to understand our product. And I think, you know, crypto, if you look at the journey, it evolves very quickly. So if you understand one piece of security technology for one CASP, you know, let's say HSM, another firm will be using MPC. What are the differences, how it works? And so, you know, understanding the technology, what kind of security layer, what kind of risks and controls you have to put in relation to all of those processes, it's quite challenging. But I have to say, I'm very impressed with all the regulators. And I think it's been a strong and challenging curve for them. And MiCAR has placed Europe at the forefront of this market, and it's really challenged all the other regulators globally to catch up.

Alireza Siadat: Absolutely, I can certainly double what you just said about the Luxembourg regulator. I also had the pleasure of meeting those in charge for the crypto asset service providers a couple of times. And I can really just double what you said. They're doing an excellent job. I mean, it's not a competition between the different NCAs. I mean, I myself am from Germany and I also know BaFin and Bundesbank. I've spoken to many regulators, but I can say certainly that the Luxembourg regulator is doing an excellent job. And there's probably also a reason why bigger players like Coinbase have decided to move their European headquarters from Germany to Luxembourg. And yeah, as you said correctly, I mean, Luxembourg as a market is already very knowledgeable and also important for the TradFi market and for the traditional investment fund market. So for crypto, I can see a strong, not just a momentum, but really a strategy where it's going to. And very pleased to see that Zodia Custody has received as one of the first players your license. And when we speak about license, we have like ten activities which are regulated under the MiCAR regime. So those crypto asset services which goes from crypto custody to crypto portfolio management. Talking about crypto custody, maybe you can just explain what kind of licenses you have and then we go specifically on the custody part and explain a little bit what kind of custody services, let's call them, so their custody is providing.

Azmina Keshani: Yeah, sure. So we provide a service and it's licensed as custody. So it's the custody license that we have. We also have a payments institution license in Luxembourg, which allows us to hold stablecoins. The service itself, so if I break it down, so when crypto started, everyone said, you're custodying the keys. You know what I'm saying? This is what you're doing. You're custodying the keys. But now, you know, I think it's quite clear that the keys are the security infrastructure. And my job as a custodian is to make sure that they're very safe and only I can manage them through multiple security layers on behalf of my clients. And that gives you access to the clients. That means, therefore, if I have access to the keys, I'm custodying the crypto assets on behalf of my clients. So that's sort of what we're doing. And they've taken it from traditional custody, which is quite different, right? So the assets are held in the central securities depository. You have an account with the central securities depository as a custodian. It's sort of like a closed loop market. So here, you know, with crypto, obviously the assets are on blockchain, they could be on public or private blockchain, but it doesn't really matter which one it is, but you're actually providing the safekeeping services. So, you know, for one of a better word, you know, we're like a lockbox provider. We're holding things safe on behalf of our clients. And that's, I guess, the best explanation. But, you know, we provide ancillary services around that. So, you know, it might be staking or any other additional services or account control services. And then of course, what's been born out of the fact that we are experts in the security of all of this is the Zodia Solutions infrastructure. Being born out of the bank, we've understood deeply what banks need and how to build not only the security layer, banks need to be able to meet their outsourcing requirements, but the risks and controls that go around that. So that's sort of, you know, how we've managed to, well, we started with custody, but of course, we've been able to develop this other portfolio business line, Zodia Solutions, as a result of our deep relationship with Standard Chartered Bank.

Alireza Siadat: I would like to go a little bit more, repeating what you said, but also going a little bit more into details. We have like those exchanges which do custody and trading. You do custody only. So this is understood. I mean, custody, I think transfer service is also with it. And because if you have the private keys, you also aren't charged for transfer outs and maybe transfer ins. And for that purpose, you also have the permission to provide transfer services. And what I was very impressed with, what you also just said, and this is something which is for us normal, but for some it is new, is that you also have the license to provide payment services for stablecoins. And this goes back to the EBA No-action letter that was basically which ended in March this year, which basically said, yeah, E-Money token at the end of the day, E-Money instruments, and if you provide transfer services to them or you hold them, you also need a license to provide this service. So it's also very great to see that you have already this license because some players are still struggling to get this. And when I say some players, it's actually custodians. So we have this on your side. And what I also want to double and to just repeat for the listeners is to understand. We have the safekeeping of the private key, as you correctly and precisely said. And on the other hand, we have the management and administration of the crypto asset. But the essential part and the security part, which also goes to cybersecurity and the critical part is how to secure the private keys and also the key recovery package, the seeds and whatever is connected to it to be able to sign a transaction or to block a transaction or to be able to take those token which you can stake and stake them and which also gives a little bit of better understanding what is possible, as you said correctly, it's like kind of an ancillary service to the typical just securing the private key and making sure that the assets are safe, but also maybe using those assets and the token to do staking and to support your customers to do staking. When I say now your customers, I think we should go a little bit more into detail, because as I understand it, like in a nutshell, you have two types of service. One service would be Zodia Custody is providing the custody for investors, like users who want to trade crypto assets, invest in crypto assets, and you safekeep the private keys and make sure that the crypto assets are safe. And then you have also the sub-custody solution where Zodia Custody is providing, let's say, in a business to business to customer relationship, custody. Can you a little bit, more explain these two different kind of custody solutions you have?

Azmina Keshani: Yeah, so I think sub-custody, it's a bit of a nuance, right? So it very much depends on the client type that we're working with and what their regulatory permissions require and where they are in their journey in relation to crypto assets. So you could have a client that comes to us and says, you know, I'm licensed, but I want to provide sub-custody. So the way that works in relation to my clients is, I'm going to deem this a sub-custody relationship, and I don't want it to be a full outsourcing relationship. And therefore, these are the requirements I need to meet. So I need you to manage one wallet for me, and I will manage the individual wallets for my client, it will be regulated by, I don't know, let's say VARA, and this is how this relationship is going to work. But because I am the regulated custodian and you're the sub-custodian, I don't have to look at outsourcing requirements and how I manage my relationship with you. You could have another entity, banks, and we typically see this from maybe larger banks that will come to us and say, well, we really need to make a large play in this market. So we have to maintain full control of the entire process. And what we're going to do is we're going to do a full outsourcing with you, where you are providing the technology for us. So that would be Zodia Solutions, we'll be providing the technology, the whole infrastructure layer. There would be some KYT, KYC requirements, but then because they're regulated and answerable to their own regulator, they would also have a doubling up of that process because they can't rely on our services there. That's a slightly different nuance in terms of the different services that we would provide. It very much depends on the client type that we work with, whether they have underlying clients or are they prop trading. It's quite a mixed bag depending on where they're going. But, you know, we are seeing that the regulated players, especially in the last year, have started to come around to, well, we've got MiCAR now. Now we've got GENIUS. Now we've got all of these regulations coming in. So we feel comfortable making a full play in this market. We also understand what we're dealing with. And, you know, this is where the regulators come in and say, you know, if you set the rules, everyone will come and they will participate in the circle or in the market. And that's kind of what we've seen in Zodia, which is why you've seen an uptick in our engagements in relation to Zodia Solutions and in our experience of working with regulated providers and supporting that security layer.

Alireza Siadat: Absolutely. And maybe let me just repeat it from my perspective, because I'm also dealing with lots of banks, which are now going to get a MiCAR license. And for banks, it's quite, I would say, easy or compared to someone who wants to apply for a new MiCAR license because they do simple notification. And there are banks like especially banks like CR credit institutions, they could notify all the ten different MiCAR services, even though they've never provided crypto custody service. So a bank can get, in the best case within 40 business days, a MiCAR license for providing crypto custody service to its clients. But in most of the cases, I've never seen it that it happened otherwise. In most of the cases, such traditional institutions like banks who never did crypto custody they would never dare to do it. So because it is a very critical service, especially when it comes to cybersecurity. And I believe that this is a very nice, let's call it like a business solution also for Zodia Custody that you provide the custody for these kind of regulated players. You don't need to, as you said correctly, have the direct contractual and business relationship with the end customers of the bank. And the bank can somehow more or less use it as a white label solution and face the customers but make sure that the safekeeping of the private keys is handled by someone who's professional in this topic and who can take care of it. And the bank can just then concentrate on the frontend and to concentrate on how to deal with the customers and make sure the customers are able, let's say, to swap their assets or to purchase crypto assets so they can more focus on trading side and leave the critical and very important safekeeping services with you. Is this understanding correct?

Azmina Keshani: Yeah, 100 percent. And I think, you know, where we sort of really pride ourselves is understanding risk, control, compliance, these frameworks, how to bring regulators along the journey, and therefore, how to bring bank clients along the journey. We speak the same language as the risk officer, we speak the same language as the compliance officer, we understand DORA, we understand banking outsourcing requirements. And we can relate that to all the technologies because we provide all the technologies, right? We understand HSM, we understand MPC, we understand all the different ones. And we obviously keep up to date as the technology evolves. And so working with the regulators and speaking to the regulators in their own language is a nuance. It is a challenge because, you know, they're coming at it from a very specific perspective. And we want to make sure they understand what is being provided and why it's the best solution or the better solution in our opinion to give the greatest security possible. And, you know, at the end of the day, the regulator is concerned about market stability. Market stability is based on, you know, safety of the assets. And when digital securities and digital crypto assets become I don't know, like a major asset within the market, they want to ensure that stability is there. So that is exactly right. So working with those regulated institutions and ensuring that they can also articulate the level of security that we provide in the language and using the words that the regulator will understand is what we think is our USP.

Alireza Siadat: What we talk about, and you repeatedly said some nuances and some topics, I want to go a little bit more into detail. So what we talk about is cybersecurity, key management, which I would say is very crucial, not just for you as a CASP, but I think where the regulator, the national competent authority is really looking at, not just when you apply for a license, but also going forward. It means being compliant when not just getting audited but really making sure that everything is safe. You touched on it. You said, you know, in TradFi, I would trade my traditional security. I have a CSD and I have a maybe a global Deed. And if something goes wrong, everything is fine because the CSD can make sure that the global Deed or the Deed itself is correct. If in a crypto environment, something goes wrong, especially if cryptocurrencies, maybe with Bitcoin, let's say, and someone is doing the wrong transfer, someone is losing the private keys, the assets are gone. So you can't do anything. You can't call Satoshi Nakamoto and say, listen, I lost my Bitcoin. Can you give me the private key or make sure I get it back? It's not really working. And this is, I think, something which, especially the traditional banks, the TradFi players did they don't see these risks. I mean, they're now all pushing into this market and they're going into this market. But I think this is very important. Therefore, I would like to go a little bit more into cybersecurity topics, Azmina. So if we say HSM, MPC, key recovery, this is important not just to the CSSF. We all know that CSSF, the Luxembourg regulator, has a very strong focus on substance, which means not just you, yourself of the company should have the manpower being in Luxembourg or in the greater Luxembourg region, but also something which I heard, maybe you can confirm that is, for example, if you used HSM, which is a hard storage model, this shouldn't be located in a third country like Switzerland or the US, or maybe it could be, but then you should have like the backup being within a European Economic Area, maybe within your on-prem location, which would be Luxembourg. If you use MPC, which is multi-party computation, this is usually in the cloud using AWS, Azure, you can also put it on-prem and put it similar to HSM on some stake on some ledger. But also if you use HSM where we have like some HSM service providers, I don't want to say the names, but some label themselves as being HSM only, which is not correct because if you would back up an HSM, you would basically do it on Azure or you would maybe do it on AWS. So there is again, not a cold storage element, but also again, a hot storage element. So I'm saying now some topics, so you can maybe go into detail to explain like from a legal and security perspective, what is the security risk difference between cold storage and hot or warm storage. And then what is very important, finally, is the key recovery. Many think, okay, my private key is with me, so everything is fine. But no, we also have to look at the key recovery package or the seeds, who has them, because whoever has them can create a new private key and can just transfer all the crypto assets from the wallet where you believe you have the private key to a new wallet. So I think these three elements are not really that clear to everyone. And I would love to hear more from you, Azmina, from your perspective as a lawyer, as a chief legal, also your custody, as someone who is not active in theory, but also in practice. What can you say about this?

Azmina Keshani: You know, Alireza, I'm so glad you asked this question because, you know, in reality, in a license application process, we spend the most time talking about this specific topic that you asked and working with a regulator to get them to understand, you know, where we're coming from. So if we take HSM, it seems to be the regulator's most favorite solution because they understand this the best, right? So they're like, okay, this is a box, it's called storage. We know where it is, so this is okay. Then of course, there's the next level. How do you access the box? When I started off in crypto in 2018, we went to places where I was told, okay, you sign the transaction, then you take a USB pen, then you drive to the mountain, and then you deposit it in the mountain in a cold storage box. And I was like, huh, how do you like scale that? You know, that doesn't make any sense. And you trust the person who's holding this? Like, what about the security, about that person? You know, can someone going to kill him and take this? And then this doesn't really work. So, you know, this is where the banking background really does help because, you know, you have to do security at scale. So of course, we have an automated solution that allows us to attach to our HSM without human interaction. That's really important. The security and the technology that we use around that is sort of pretty high grade technology that creates that process. And then you have to explain why did we use that technology? How does it work? And why is it of a specific grade that makes us comfortable that this is still cold storage? Doesn't mean warm storage is not safe because the way you access warm storage is the key point here, right. You know, you have exchanges operating billions of dollars using hot storage. And, you know, for all intents and purposes, assets are generally managed in a way where you don't hear of many loss issues. So losses happen in quite unique circumstances. So not necessarily just because something is in warm storage or hot storage, it's the security protocols around it that you have to focus on. So I think these things are quite interesting and different regulators are in different parts of their journey in relation to the different technologies. And I believe that they're coming on that journey with us. And I strongly hope that we can bring the regulators on the MPC journey, because I think that is something that we're confident in terms of the security, how it works and how we manage the MPC security. But again, it's a bit of a journey with the regulators. At the same time, I love those conversations because they really challenge our thinking, well, how do we explain it in a way that, you know, works for the regulator? What is it that we're not saying in the right way? What are we not explaining, right? Because, at the end of the day, it's in everyone's interest that we all understand the technology and how it works. But key recovery, okay, so I'm just going to address that. Key recovery, this is obviously our most secret process. So I could tell you, but I would kill you afterwards, how we do our key recovery. It's a complex process. It's a very important process. And, you know, it goes to the crux of how the security of our keys and how we recover the keys.

And, you know, the time that we spend in ensuring that process is secure enough with our auditors as well is fairly complex. And I believe everyone would be going through the same process, right? It's a security issue for the process. It's a security issue for the individuals that are involved. It's a security issue for the regulators because it goes again to market stability. So very, very interesting thing to go through, I would say, and something that everyone should really spend some time in understanding.

Alireza Siadat: Absolutely. I think what you said is very important also to our audience. There are some regulators. I think the Hong Kong regulator is not comfortable with MPC only and is asking to have the key recovery being on-prem and some service providers in the market who are normally strongly focused on MPC have now also introduced the HSM for the backup or for the recovery, yeah. But I myself, I'm similar to you, I mean, I'm also a big fan of the MPC, especially if you have a strong MPC. And if you use then Azure or AWS with an encrypted security backup, why not? So unfortunately, we now all are aware of the wars happening in the Middle East and what could happen if you have a war. And in that case, I would argue and say an HSM is not the right thing. Or if you have some pandemic like Corona or some other catastrophic things happening where like physical storage is maybe not the best, but I'm not here to judge. I'm like, you're only a lawyer. But I think that if we talk to the regulators, which I also do a lot, similar to you, Azmina, and we explain exactly why MPC is good, and why also maybe a solution only model where you provide, as you said it, the Zodia Solution as the infrastructure powering the custody rather than providing custody. This is not custody. So this is only the solution. And maybe you explain a little bit going now back from cybersecurity to your second product, which is the Zodia Solution. What does it mean in practice? The distinction between you providing custody or you making the bank being able to use your solution and providing the service by itself?

Azmina Keshani: Yeah, that's a great question. So, you know, we're a custodian, we are the regulated entity and we have regulated entities in seven jurisdictions globally. And what that means is you are responsible for safekeeping the assets. You're responsible for overseeing the security and the controls and the processes to ensure that the whole structure works. When you are the infrastructure provider, that responsibility and that liability sits with the regulated provider. The solutions team and the Zodia Solutions product is we provide the technology which helps you meet your regulatory requirements. And you always maintain the control over the processes, the oversight over the processes. And because it's an outsourcing, you would have the right to audit, come in, look at the technology, see how it works, and ensure that we're able to meet your regulatory requirements without having to, I think the best way to say it is that there's a technology, which is the wallet technology, and then there's a layer over it, which is the risk and controls that sit on top of it. We've already built the risk and controls, which allows them to monitor and manage that in a regulatory way that meets the regulatory requirements.

Alireza Siadat: Thank you. I think that this differentiation is very important for those who understand, not just those who want to become CASPs or want to provide crypto custody solutions, but there are also some regulators sometimes listening to our podcast, especially from those jurisdictions where they now face newly applications. And I think this is very important also to be shared with the audience. I would like to go a little bit in the remaining ten minutes we have to what you said also in the beginning. When we speak about crypto custody, it's not just about you have the license to provide custody. That's why you only safekeep the private key. And this is how you make your business, your profits. I think what we need to understand is that it's not just buy and hold. It's not just buying Bitcoin and holding it and selling it for more later and making a profit if it hopefully all goes up. Nowadays, you can do much more. And you touched on it, you said staking. And I have like two examples which I wanted to share with you. Starting with the first one, how do you see automated swap of stablecoins? We know that stablecoins are E-Money instruments, which means E-Money is not allowed to pay yields to the holder. So if I would have the E-Money token, the stablecoin, I cannot get from my bank or from the issuer, yield. This is not possible. At the same time, bigger players like institutions or banks would love to have their Fiat funds in digital assets like E-Money token to have a good treasury management if I want to do cross-border payment or they want to use those stablecoins for something else. So what I see in the market and this is what interests me to see what you say about this is that they take their stablecoins and they can then swap it against yields bearing instruments like Tokenized Money Market Funds or maybe even Commercial Bank Money Token which pay out yield. How do you see it as a custodian? Where is Zodia Custody coming into this? And I just want to give one more bullet point, which is a smart contract maybe, which is set up and realizes that the stablecoin is coming from wallet A, going to the issuer of the Tokenized Money Market Fund, and then the Tokenized Money Market Fund issuer is minting this Tokenized Money Market Fund, the token, into the existing wallet or into the original wallet where the stablecoin is coming from. So basically a smart contract would say, whenever a stablecoin is coming from this wallet to the issuer, the issuer is going to issue automatically the Money Market Fund into the wallet of the issuer. And then you say again, wallet and wallet, which has a big custody element. So how do you see this?

Azmina Keshani: I think you've stumbled upon a regulatory challenge right there, Alireza, which is one that I think all the CASPs are contending with right now. So Money Market Fund and a digital Tokenized Money Market Fund, whether it's digitally native or otherwise, is likely to be deemed a financial instrument or a security in a number of jurisdictions in which we operate, in which case you would need to be able to have a license to hold the tokenized security which is not covered under MiCAR. Under the UK rules which will come into place in September, we're told this year, we will see the issuance of that, of the finalized rules, they cover specifically a separate license for the safekeeping of the tokenized securities. So in the UK, something like Money Market Fund and digital version could be deemed a financial instrument. So when you're swapping, you're covering different regulatory parameters. So I mean, what you say in terms of technology is kind of easy, right? Like anyone who has the technology, any custodian, any exchange and any CASP can do this. Building that technology, it's not on a big uplift. We can do it with each other. We all know this. It's just making sure that you have the right licenses to do that. And then when you're looking at the regulators and what they're thinking about, they're sort of trying to create the parameters for people, banks, crypto asset service providers to be able to interact with each other with different asset classes. But of course, I assume, you know, probably tax legislation hasn't caught up with all of this. Another layer that has to be considered and managed in relation to all of this. So, you know, if you're swapping a stablecoin for a Money Market Fund, then, you know, what does that mean? Who's managing the tax in relation to that? There's a number of different things that, that fall in and around that we have to consider in the ecosystem that is being built to that, you know, the different crypto asset service providers are building with each other, the ones that they're building with the banks as well. There's definitely synergies for all of these providers to work together. And I know what I can say to you, we're actively working in the market to build solutions like this and to make it work. But I think that in terms of the regulatory journey, there's a little way to go to make it a reality.

Alireza Siadat: Absolutely. I mean, you now touched on the UK regulation, which is now getting, I would have said, closer to MiCAR, but they have their own regime, starting with regulating or putting a sandbox for stablecoins and now going more into the digital assets or cryptocurrencies in general, and then also combining both elements, as you clearly said, the regulation of crypto assets with the existing MiFID of the regulation of the financial instruments. And as you are in Luxembourg, and Luxembourg is pretty known for the fund industry, I believe that we will see you, let's put it like this, rather soon. I don't have any insights, but I believe that we're going to see you rather soon also taking care of not just stablecoin custody, but also Tokenized Money Market transfer, which are set up in Luxembourg. And then you have this swap element coming in. I personally you see this as a strong market, not just because of Franklin Templeton and others who have put their Tokenized Money Market Funds, but because big institutions, big banks who come from TradFi, who are big into treasury management and how to get yield, I think they're all looking right now what you can do combining these two worlds, MiCAR and the traditional method world, which is going to be very exciting. But let's go to another topic. You touched already on international harmonization or leveraging international regulation. You talked about UK. I want to look to the big elephant in the room, which is basically the US market. So we all know, or most of us know, that we have the GENIUS Act, which basically is, again, a sandbox for stablecoins. And as I understand it but I'm not an expert under US law. I just have good colleagues with Deloitte in the US, who told it to me in that way to say, if you apply for a GENIUS license, let's call it, or for GENIUS permission to issue stablecoins, you could do that also from Europe with your MiCAR license. If you're regulated to provide or to issue stablecoins under the European regulation, you could easily upgrade or notify the US and then also be able to not just issue a MiCAR compliant coin, a stablecoin E-Money token, but also a stablecoin in the US. And now my question comes to you, how do you see that? Can we combine like MiCAR and GENIUS to leverage it, custody of stablecoins, which are regulated under MiCAR and also custodying stablecoins under GENIUS Act, like from your perspective as a custodian who's active globally in different jurisdictions?

Azmina Keshani: So the custodian is regulated by the regulator and the jurisdiction in which it provides the services. And in the US, it's fairly complex. I mean, the GENIUS Act and the Market Infrastructure Bill, which we hope will be coming in, is helpful as it's providing quite a lot of clarity. The OCC in the US has come out and they're providing licenses to banks and they've already given permission to banks to hold and be custodians for crypto assets and stablecoins. I think combining the two, I think is interesting. I think what we will see, there is a proposal between the FCA and the SEC to create a US-UK digital asset highway to test and work out how we can manage the movement of these assets between jurisdictions in a compliant way and without triggering any, so there could be currency restrictions or tax restrictions that would apply in relation to US assets. There are a whole bunch of restrictions on that, which are sitting outside of the GENIUS Act, which would apply to these assets that have to be considered. And I think that by implementing another highway, so another sandbox between the US and Europe, which I think is important, is how we're going to work out how this all works in reality and then build the regulations around that to ensure that it's compliant in that sense. So it's difficult. So I think, you know, in our minds, you know, we know how to do it and we want to make it happen. And we think that this is a global economy and this is how we should be thinking about transferring of assets, making business easier in that respect. But there is little way for us to go together collectively. And, you know, I see the leadership of the SEC in this. I've seen a lot of changes, which is fantastic for us. And I think if you bring that leadership together with what we're seeing in Europe, I think we'll see, and in the UK, we will see great changes happening in the not too distant future.

Alireza Siadat: Very interesting. Also, the highway solution, as you described it, between the UK and the US. Let's see what is happening there. And it's going to be definitely exciting. This brings us to my last question for this podcast, where I want to touch a little bit again on how banks can tap into crypto and crypto custody, crypto trading. I mean, I was speaking to banks a long time ago, like four or five years ago, especially German banks, where they were saying, we're going to do everything by ourselves. We're going to build up our own custody solution. We're going to build up everything by us. This is how it works. And then on the other side, you have those crypto exchanges, those crypto firms where they already have like some nice solution in place, some really good working solution, custody solution. And I was a couple of weeks ago in a Nordic blockchain conference where Nordic banks were now also tapping into crypto, were telling me, oh yeah, we're going to do it by ourselves. We're going to build up our own crypto custody solution or we're going to partner with another bank which has their own crypto custody solution. And I was like challenging them. I said okay, what do you mean with building up your own crypto custody solution? Are you going to like build up your own MPC or are you going to use an MPC provider? Because I know that this bank who you like refer to is using the following MPC provider. And I said, yes, yes, I mean, they're using this MPC provider, but we're going to put our own layer on top of that. I said, okay, honestly, I don't really understand it. But bringing it back to my question and like giving you like this background, this scenario, Azmina, so as most digital asset infrastructure was built originally for crypto firms like crypto exchanges, not for banks, not for traditional banks, does that origin actually matter? And how should institutions like banks weigh the choice between building their own solution, which I would say is not really working, buying something or maybe partnering?

Azmina Keshani: So I don't think they could really be building something. I mean, they're not experts in this area. This is not something that they do. It's like, you know, I'm not a great cook, but you know, it's like telling me to cook like an amazing dish. And obviously it's not something I'm going to be able to do very well. But, you know, banks have to maintain the highest standards because they have prudential requirements and they also have all these regulatory requirements to ensure that they keep assets specifically safe. So really they should be working with a provider, pick your provider, there's many out there, and you know, ensuring that they understand, they have to, they have a regulatory obligation to understand the technology in minute detail. It's not like they can just pick it up off the shelf and implement it. They need to hire people who understand the technology, explain it to their senior risk officers, build a plan around the security in relation to that. They're going to have to add layers onto that to ensure it complies with their own regulatory requirements, any controls in relation to what can happen, when it can happen. And then they're going to have to integrate that into their own systems. So that's the next layer. So it's a whole bunch of other people who know how to do that, to integrate it into their systems and then integrate it into their own reporting requirements. And then compliance, KYC, KYT, who are they using? How are they going to integrate that? How are they going to integrate that into their global and group reporting? What is the process around reporting to the national crime agencies? How are they going to implement that? Do they understand what the risks are? There's like, it's a minefield and you like to need to build out a whole department team who understands how to do this, right. So, I mean, I'm not saying the banks are far off. I would say some banks are further ahead than others. You know, some have already built their own solution. But when I say built, they bought the technology, they worked with the technology provider to make sure they have a compliance solution. And so I think that those ones are further ahead. I don't think, I mean, maybe I'm being a bit cynical, but I don't think it's easy for a bank to build this by themselves. They're not technology providers, and they do need to work with those technology providers to build this in a way that would be compliant. But also, I mean, I think the other thing to bear in mind is they have so many constraints in what they can develop and how they can develop it. They don't have the ability to just go, okay, let me just try this out and see if it works in the same way as a technology company, because in our company, we sit around the room and we're like, how do you do this? Let's do this. Let's try this. Let's like spitball. In a bank, everything has to go through a controlled process while they're doing that, right? You know, I'm not saying they're not innovative, but they do have restrictions on how they can innovate.

Alireza Siadat: Absolutely. And I wouldn't say it's either or. And I think that's the nice thing about the digital asset or crypto asset environment that, as you precisely said it, you can let the crypto final expected in crypto build the product, build it fast. And to be honest, behind all great tech companies like Zodia, there is a bank in the background. So we have a few Standard Chartered, we have with some other banks in the background. And as soon as the time is coming, you can then partner, you can work together. And I think this would be a very nice outcome for a win-win solution, basically. And with this said, Azmina, it was very insightful speaking to you. Thank you. And I think also our audience is happy about this first English-speaking podcast. It was lovely having you with us. Thank you for this. Yeah, and also thank you to our listeners.

Azmina Keshani: Thank you, Alireza.