Legal on Air – Der Steuerrecht Podcast von Deloitte
Episode #29: „Krypto verstehen – Folge 16: DeFi Compliance“
Speaker: Alireza Siadat, Hedi Navazan

Alireza Siadat: Welcome to a new episode of “Krypto verstehen” or as we say it in English: “understanding crypto”. Today I'm very happy to have a guest with me, a special guest, for the first time a lady who is on maternity leave. So, thank you very much being with us, Hedi. Can you please introduce yourself, who you are, where you are coming from and what is your relationship with crypto?

Hedi Navazan: Thank you so much, Alireza, for having me today. Happy to be here and hello everybody. I promise it is more fun than it sounds. If you fall asleep at this, you will wake up compliant. So, my career has really been about sitting at the intersection of traditional finance, digital assets, technology, working with regulators and law-enforcement agencies. I've been advising governmental bodies and international law-enforcement agencies and led complex cross-border investigation. I've seen that intersection from very different sides in my role from the boardrooms of Dutch banks and HSBC to blockchain analytics at Crystal Blockchain and then serving as the chief compliance officer at 1inch decentralized exchange aggregator, where have been operating from inside the ecosystem. Today also serving as a senior advisor for global compliance and enforcement at GBBC, I get the chance to bring those perspectives together, connecting industry, regulator, and law-enforcement. Alongside of all that, I took on my most demanding role yet, mom to my six-month-old baby. You know, compliance taught me patience, Alireza. A mother who is testing whether it was real.

Alireza Siadat: Thank you so much also Hedi for being with us. I know it is tough to manage such duties. I mean I have myself two kids, but my wife is supported me, so thanks for that. But yeah, being with us on the podcast and sharing your really, valuable insights and it is difficult to find someone who is or was active in TradFi and then also in DeFi, so decentralized finance. And I know for long time I remember back, I don’t know, ten, 15, maybe 15 years. When we both were also dealing with projects related to Iran so really know the tough sanctions and compliance stuff and now being in crypto. So, it's very nice having you today as my guest on my podcast. So, my first question with your background would go into the direction of what is basically crypto AML compliance. I would personally say it's the same as traditional compliance, but you can dip into that. The global AML rules sat as the FATF rules apply in the same way to DeFi or to crypto as they would do in TradFi. But at the same time, I would say it's different because in crypto we have specific tools which you need to use which are not familiar to those in TradFi. Can you elaborate a little bit on that?

Hedi Navazan: Sure, absolutely. I mean, let me be bold about that. “Same risk, same rule” - many believe in that. No, I don't think so. In 2022, when I was at European Parliament, just before MiCA bill draft was being finalized, the banks lobbied heavily against crypto. Their argument was: “Why do we have to go through strict rules? Why crypto companies don't? Same rules for everyone.” I

understand the frustration, but we are talking about a completely different foundation as we mentioned blockchain. People who truly understand blockchain and TradFi, they know these are fundamentally different by nature. To give you an example in my previous roles, I monitored thousands, thousands of transactions within the financial institutions. I set up monitoring systems, procedures, compliance team of the filing SARs, suspicious activity reports, with the FIUs. And the reality is within the banking system, these transactions were only visible, only to us, the compliance team and not even everyone in that team. Authorities outside had no direct view. Still today, that is how it is operating. They only see what we choose to report. I had raised red flags on famous multinational companies that I cannot name here. You will have to maybe, wait for my memoir, like I saw your transactions, but you know on a public blockchain, the information is public to you, to me, society, to authorities and I know what people may say, but we don't know who is behind a wallet address. Of course, we don't and we should not. That's privacy, it's security. Otherwise, people get kidnapped. But what I'm trying to say here is behavior and patterns are detectable on-chain. It's public to everyone. If something is going suspicious, authorities can see it. Immediately. They can reach out to the crypto exchange where the wallet is hosted and ask for the details about the individual or an entity. One might say, oh, so you are saying we don't need rules. No, that's not what I'm saying. What I'm saying is we need rules built around what the chain gives us. So, my question is here, why do we need identical rules, like travel rules or minimum thresholds when so much of the information is already out there. It's like, for me, it’s like asking someone to submit a written report about the weather while you are both standing in the rain. What we have now is same rules, different reality in banking transactions sit behind the closed doors on blockchain scene is public.

Alireza Siadat: I like that very much what you're saying and I'm not sure how familiar you are with the German regulator and what was happening in Germany, but it was like the German president of the regulator BaFin, Mr. Branson. He said, in some big newspaper, he said blockchain and Bitcoin and other crypto assets are used by criminals and for criminals because blockchain and crypto is anonymizing the token holder. And then there was like after that one day later a big German newspaper made to chief guy this German newspaper made an announcement like an interview said no give you like a reply to that interview saying no. Blockchain is not anonymized, it's pseudonymized so it means that what you say exactly it's transparent to everyone, so everyone can see the wallet addresses and where things are going, but you don't see the clear names. You don't see who is the owner of the wallet, who is controlling the wallet, who is having the private keys and this is exactly what you’re saying. And this is also the rule why probably blockchain-related transactions need to be also handled different in different rules maybe are needed. And if we say this, I mean what may don't understand, especially the regulators, not just the German regulators but regulators in general, especially their AML and compliance departments. How you can see a blockchain transaction and for that a tool is important and you being like active on all sides and also being active of crystal analytics. Can you explain how does a forensic tool work like from a perspective of an AML officer? And maybe also from the perspective of the managing

director of a crypto exchange, crypto service provider? Because this is probably different, but maybe you can explain it for us so we understand it for those who listen and never used a tool.

Hedi Navazan: Absolutely, Alireza. As you very well said, you know, forensic tools are very advanced nowadays. Having blockchain analytics in-house is almost a must-have. Tracking the transactions manually in this scene with that blockchain analytics is almost impossible and exhausting. You know, imagine doing it with a spreadsheet and a strong coffee. I've seen people try and believe me it doesn't end well. Blockchain analytics how basically they work and the mechanism behind is they cluster addresses using heuristics and machine learning and they categorize them. Then with the access to data and intelligence they label the wallet addresses. For example, this one may belong to an exchange. This one looks like a hot wallet of an exchange. The other one is associated to a scammer. There is another one sanctions-related or one other address look like or the clustered addresses look like a label for mining service. But, there is a but. Here is my golden rule. It must be evidence-based. I've been on both sides as you mentioned, I helped shaping the industry at the blockchain analytic firm and I used these forensic tools myself as a user, when I was the CCO of 1inch. If analytics tell me an address belongs to a scammer, I would not act just because of that. Show me the evidence. If you label an address as sanction, show me where the data comes from. And yes, has that been a problem in the industry? Yes, it has been. There was a time, analytic firms labeled addresses based on public reports. They opened the auction on the platform, asked the society, yeah, report addresses to us, but that's not correct because anyone can start the campaign and report an address as a scam. By that logic, if enough people on the internet say your neighbor is a vampire, he's a vampire. You know, there are another example I have seen real life that sometimes you see like analytic firms put addresses mentioned in a court ruling under the sanction category. I heavily challenge that back in the day because in compliance, sanction means you freeze assets. Imagine a compliance officer relying only on a wrong label and freezing someone's assets, its people's money we are talking about. Imagine what happens to people's money, but I would say a label is a lead, but it's not a verdict. You question about the director of a firm or MLRO, how do they use these forensic tools? What do they need to know? I mean, if you are a managing director, I think you do need to know that analytic, like blockchain analytics is a powerful starting point, but this is not a substitute for judgment. MLRO needs to know how the labels are built, what evidence sits behind them, and when to challenge the vendor, I have been challenging the vendors when I have been seeking as the CCO in other roles, politely, but firmly give me the evidence. But I also like to share if you maybe you have similar experience, Alireza, as well. I have also seen at some you know exchanges and many, we still have immature teams working in support functions at compliance and you know this is true. Many crypto exchanges have teams experienced in TradFi, but not in crypto, not in reading transactions on-chain, not in blockchain investigations, and their decisions have a big impact on people's assets. I have a personal experience myself. I was transferring funds from my asset at an exchange to my own private wallets. They ask me to prove that I owned the wallet. Fair enough, that's legitimate, check. But can you imagine what they ask for?

Alireza Siadat: It is hard to imagine. Normally that you would do is a Satoshi tests or the electronic signature if you're in crypto, but if you not in crypto, they probably would come up with asking you for the receipt from the wallet where you bought it, something like that.

Hedi Navazan: Very close. They asked me to write the wallet address on a piece of paper and take a photo of myself holding that paper next to my ID card. I was shocked and you would be shocked if I told you the name of the exchange, I won't, but it's one of the biggest players in the world by the users and volume. As you said, you prove you own wallet by signing the message with it that's the whole point of blockchain, cryptographic proof, not a craft project, and a person who understands the technology knows this in five second, as you mentioned, you know, on a blockchain, you don't show your paper, you sign your proof. So yes, it is a knowledge gap. I would say you cannot investigate a blockchain with the bank's paybook alone and it's like to me it's like navigating Madrid with the map of Amsterdam. Lovely canals, wrong city. Although I lived in both cities, but yeah, it's not the same.

Alireza Siadat: It's crazy. I mean, I think we're one step too fast for the ordinary listener. We have also have sometimes people listening to this podcast who work with authorities. So, just to give an example, I mean what the tool can do in simple words. A forensic tool can tell you where the transaction was coming from. So, looking at the transaction where the transaction was coming from, but it's much more powerful. It can even tell you where it was coming from before. So, the hops, we call it the hops before, you can go ten, 20, 30 hops you can connect. Very nice image to say where is the crypto asset really coming from even after what's way it's going to and to give you like an example, it's a true case example. You have heard it in the news that somewhere saying yes in this new conflict between Iran and in the US that the mullahs were transferring out crypto assets out of the country using some European banks and some European regulators took this information which was in a newspaper not a proper good newspaper with solid information as you say like a witch hunt. They were taking this information and basically going to all Iranian banks in Europe and asking them for, yeah to show if they were involved in this crypto transfer activities and in my opinion and I would like to hear your opinion about it. Basically as you say, just go on the blockchain, you can go for Bitcoin, you can go on Ethereum go on a Etherscan, go and scan the transactions which you think were coming from Iran and look to which wallet address it went, and then try to find out who's the owner or the controller of that wallet address, and then you can find it, you can see who it is, but how would you tackle that with a forensic tool in such an example, Hedi?

Hedi Navazan: Yeah, 100 percent. I mean, I'm again surprised by these practices and look at me, we are all here to learn from one another. So, but we have today's very advanced forensic tools. Blockchain analytics are also much more advanced than six, eight years ago when I was active in this space and it's so easy that you can just check a transaction on-chain. Even if you don't have access to blockchain analytics which are normally paid services, you can just check it to yourself and you can see the wallets that have been linked to that transaction. And what the beauty of blockchain is, it's immutable, it's transparent, you cannot change or edit or hide or remove that

transaction. Let's not forget these things has happened within the banking system because that stays within the bank authority and ownership, but on blockchain, we cannot alter anything. And as you very well said, what I like as well is that you can just go hops back. By hops we mean, like you go one transaction back, one transaction, it can be indefinite. However, there is no point of looking indefinite because it becomes very difficult from investigation point of view to leak something that has maybe 50 transactions behind to what is currently happening and link to that transaction under the question. But I think what we have even now, even have AI adding to the blockchain analytic tools and some of them are empowering their capability. Just investigation has become much more easier and much faster by using AI characteristics.

Alireza Siadat:: Absolutely and I mean remember back in the days we both went to some Interpol event in Lyon it was and this year I was in an Interpol event in Vienna and I met an Israeli company, which is doing auto forensic services and they're combining on-chain and off-chain data so that basically are able to track with the on-chain data the wallet, the wallet address and connect that wallet address to device like a smartphone or to computer and once they have that information, they can find out through the activity which this device is doing online like going to web pages, to social media, to other things, to find out the profile of this user, to find out where this user is moving. So of course, you can cover your address by VPN blocker and stuff like that, but once you use the device like the smartphone, the same one with where you have the wallet connected to and you go, I don't know, you go on a social media platform and then you start being active there or you start ordering food from somewhere. Then your profile becomes more more transparent and this is something which like now the authorities who are active with Interpol relies and see, but unfortunately some the regulators don't see it. This is a pity, but it really fits in also what you say about how to combine AI with these tools and to make more out of it. And really coming back to what you said in the beginning, I also believe that the blockchain itself is a very good tool from AML compliance perspective to have a transparent view on users, transactions and to really, as FATF said a long time ago, to really leverage blockchain as a tool to be compliant. With this said, I want to understand how being compliant actually works in something you did also for long time being active in DeFi. So, the background to that question goes a little bit to what we discussing so far is that sometimes you don't need information. As you said, if you stand in the rain, you don't need to write a report that its raining, people see it. So, what I want to understand is how DeFi players like 1inch, Uniswap and some others aiming to be AML- and CFT-compliant when they do not have the same means and access as centralized players like they usually do not do KYC in the beginning. They usually do not have the passport copy of the user. They usually do not have the last invoice of the electricity bill and stuff like that, but as I know from what you did at 1inch, and it's that public knowledge that is published on 1inch website, 1inch shield and so on and so on, there are many other means which you can use to be compliant. So can you explain to the listeners also those who always say that DeFi is not compliant how compliance AML, compliance works in DeFi.

Hedi Navazan: Sure, absolutely. That’s a good point, Alireza, I was recently asked in an interview, does DeFi even need AML and CFT and you know the look on people’s face. They say isn't the

whole point that nobody's in charge because that DeFi that decentralized. My answer is yes, nobody is in charge, but yes, it still needs a certain, you know, frameworks on AML, CFT, but it should be proportionate and even though it is decentralized, it still facilitates the movement of funds through a platform, one way or the other. And I think from my other experience and 1inch, what I would say here is, if you ask me, what is the biggest risk in DeFi for me, the risk in DeFi is more towards cybercrime, hacks, exploits, wallet draining, you know MEV bots, not sanction or terrorist financing. Everyone talks about sanctions and terrorist financing because it's easy to sell. It's easy for my grandma to understand, but the real everyday threats are smart contract vulnerabilities as we call them more sandwich attacks, phishing, drainers. And as you mentioned that 1inch, we had robust security measures in place. We blocked addresses linked to scammers, bad actors 24/7. We were also using blockchain analytics as well. We were monitoring screening around the clock. We were not alone any bad actors to use the platform for their malicious purposes and still hacks and cybercrime remained the top concern. Why did we do that? The question is here, because the regulator asked us to do. No, there is no regulation on DeFi because we cared about a safer ecosystem. We do not want to facilitate bad actors misusing the platform. We want to take care of other users. We want to take care of, you know, consumers and I do think consumer protection is crucial here and the only thing in DeFi what I can say is that works 24/7 without a day off is the hackers trying to drain your wallet and the compliance team. We don't get the weekend either proportionate doesn't mean it's optional. We have to take actions and we had multiple forensic advanced tools at 1inch making sure that the platform is not being misused by bad actors. You mentioned about a KYC copy of the passport. Yes, DeFi platforms they are not asking for KYC of the users because most of the times these users are linked via a centralized exchange. Yeah, so the centralized exchange has the KYC on those users. So then there's an investigation going on and I have been collaborating a lot with cross-border law-enforcement agencies. We know which exchange has been facilitating that user and we can show the name and the authorities go to the centralized exchange asking for the information of that user. So, this is one way how investigations have been done and run with decentralized exchanges and although there is no regulation. But does it mean that we should allow being misused by bad actors, by scammers? No. And at 1inch, I'm very proud that the firm stepped in and that is the legacy of the 1inch that building a safer ecosystem and truly the team cared about this matter.

Alireza Siadat: Yes, I mean absolutely what you say about KYC. KYC stands for "know your customer", but I'm trying to be bold and I'm trying to make a statement, and I try to see how you react to that. For me, KYC or "know your customer" is not up to date anymore. For a simple reason: Nowadays we do KYC because we want to know the identity of our customer. Why do we do that? We take the identity of the customer to have the profile to see how this customer is doing transactions, how the behavior is, how the profile of this is. But what we do in the beginning, we take the maybe take the name and run it against some sanction lists because the sanction list tell us Mr. X is a bad actor. So, we didn't say oh we have a hit: Mr. X is a bad actor. Hmm, I cannot deal with him or more maybe Mr. X is a politically exposed person oh, I have to apply and have due diligence. Sometimes, many times Mr. X is not the right Mr. X because my Mr. X is a different Mr. X.

So, this is a wrong hit. So, a fault hit and this helps a lot because data which you have in this kind of traditional tools they're not up to date they're very old and they're not usually updated that fast and you work with old data. So, what we do is we collect data, we check data against existing old data and then someone is telling us this is a bad actor and then we say, okay, we cannot deal with this bad actor. But we don't really know if this person is a bad actor and how this person is really acting. So what crypto is doing in my point of view and what DeFi is doing very well, is not looking at the name and identity of the person. It really looks at who is owning the account, who is owning the wallet and is the owner of this wallet a bad actor because what this person is doing. So, we connecting incidents, incidents which we are aware of. Crypto players are sharing this data with other crypto players to make sure that this bad actors are not going from one place to another place to do other stuff. And this is why I believe even though DeFi has a lack of not knowing the true identity of the persons, but it is much more advanced, much more sophisticated because it has much more information where it is really looking at the profile at the bad actor. So, this is my opinion, but giving it back to you, what do you say about my analysis?

Hedi Navazan: No, this is absolutely spot on. I would love to share actually an initiative in the DeFi scene that we were part of setting up: war rooms. Call it war rooms and meaning the industry, the ecosystem share the information right away on spot with one another to protect at the end the platforms against being used by the hackers in this case. And this was a proposal I shared actually in August at symposium at Cambridge as one of the initiatives in the industry that can be taken and DeFi players have been much, much proactive in that sense. And I can give a example which is a public information anyways Bybit hack, which was one of the biggest hack thing in the history of crypto by far. We have been acting in that war room and the moment that they hack just a second that this hack happened, we were receiving information directly right away from Bybit team. We were already ahead of the time blocking all the addresses of the hacker against our own platform. I'm very proud to say that around 720 addresses were already blocked by us at that time by 1inch. Perhaps it was around, but please don't quote me if very few minimal addresses were not blocked that the hacker could swap the funds, but it was very minimum. Yeah, we did it. We had tools in the house, we had invested in forensic tools, we were cooperating, we had these war rooms set up with other industry players. And that is how we were protecting the rest of the, you know, ecosystem. And as you said these such examples, I have never, Alireza, seen in the TradFi. I have seen the opposite example during my time. I remember they received letter from authorities one of the you know accounts were linked to a scammer, we were, we took action, but the same scammer had an account in another bank. You know we could not talk to, the banks don’t talk to one another. They won't share information obviously because of privacy reasons and security reasons, but we see a totally different scene specifically with DeFi players.

Alireza Siadat: I mean, yes, I mean, absolutely. This is what I also admire. And again, also here again, the technology, the blockchain helps also to be fast, to be very fast and to share information and to make sure that bad actors as we call them in DeFi are not successful in offering the stolen liquid assets and this is very important. And just to give you another example before I go to my last question, to my last topic, you can pretty much see how bad or how old-fashioned traditional tools

are when we look again at your other favorite topic, verification of self-hosted wallets. So, the verification of self-hosted wallet even if we do it by signing a transaction, this still does not say if the person who you KYC and you have his identity is really signing the transaction. Because if you would ask me, Hedi, you would for example be the Chief Compliance Officer or AML Officer of a famous crypto exchange and you would ask me to sign a transaction with my private key. You wouldn't know if I do it if I would call someone and tell this other person please sign a transaction. You don't know it and this is the simple thing and this is how I would also say not just in DeFi, but also in TradFi, we're identifying the person who first talked to us and who we think was owning the account and using the account. But what if ten, 20, 100 people are using that one account, which could happen and it could happen in TradFi, it could happen in DeFi because we only identify the person at the beginning and try to follow and track this person during their lifetime. But crypto is different. For example, I was giving examples of DeFi or know how they set up a profile of a bad actor to use maybe that to do self-hosted wallet compliance or I also wrote the paper where I said if you really want to be secure you need to use a biometrical data and you need to have the biometrical data of the user in the beginning to make sure that every time that the user is signing a transaction it is this person who you identified in the beginning and match the biometrical data like fingerprint, face recognition, whatever, but I wrote the paper on that it was not really used in public and practice. It is out there, but yeah, coming back to you from your experience, long-time experience. How would you do with a self-hosted wallet some verification?

Hedi Navazan: Actually, you give very good practical solutions. Even this is about self-hosted wallet verification. Maybe it's very controversial, but why do we need a self-hosted wallet verification? What I'm trying to say is this question, for example, the example that I gave to you is I think it was the personal example, but generally what maybe the regulation had asked now the crypto exchanges to verify at the owner of self-hosted wallets because they consider self-hosted wallets risky, and I'm very bold about that I'm not in favor of that. There must be multiple, multiple factors all together to make a self-hosted wallet as a risk factor and on the verification itself. I mean you gave very good practical examples, the fingerprints and the face recognition, while the individual is signing the transaction. I think these can be in practice used, especially with the technology that we have. But as I mentioned more and more, I feel that sometimes compliance teams are not mature enough and do not tech-driven enough to leverage from the availability of the tools and the practical solutions we have in their space to use if it's needed to verify your self-hosted wallet. We can use this mechanism.

Alireza Siadat: Absolutely, now coming to my last topic, which is also, I would say for the closing a rather controversial topic again. We all from the crypto environment know the Tornado Cash incident let's call it, but for those who do not know it. Tornado Cash is a tool with which you can basically cover the trace of your crypto transaction. You can call it the mixer where your transaction goes through and no one really knows where it was coming from and where it is going to. And it's a tool used I would say 90 percent by legal activities like people who donate money even Vitalik Buterin was donating money to some initiatives in Ukraine who didn't want to know that people know from where it was coming from because as we said in the beginning, blockchain

data is very transparent, if you know the wallet of someone you can see exactly how much assets this person has, what this person is doing, but if you don't want others to know what you doing, you would use something like Tornado Cash to give you the privacy which you need in this kind of world. It's basically, compared to the real life, is using a car, driving in a car with black mirrors because you don't want other people see you in public and which is not illegal, but also Tornado Cash was used a lot, not the majority. I said 80 percent legal, maybe ten, maybe five percent, maybe I don't know the right number, but some illegal activities like the North Korean Lazarus Group who used it. And then what basically happened **t**hey put the web page tornado cash in a day with U.S Treasury's OFAC on a sanctions list. And one of the founders of tornado cash Alexey was living in the Netherlands, like also your former homeplace, Hedi. They put him in front of a court and the lady judge did not really understand who this guy is, thought that he is a manager director of a criminal company and it was a big case around him and in the end of the day he got out of prison, everything was fine. Tornado Cash was delisted from the US sanctions list, but many people, many do still say Tornado Cash is something bad. So, my question to you: Is Tornado Cash by default bad and do you have any insights from the US? I think FinCEN has some activities there, US regulation has some activities there. Do you have any insights what is happening from the US perspective in that respect?

Hedi Navazan: Sure, I mean you touch on the most controversial name in space to an ether cash and I would like to share the very recent, it's just two weeks ago, this announcement came about the action FinCEN, the Financial Crimes Enforcement Network of United States, took to redraw its proposal on mixing services in this case Tornado Cash, but also on self-hosted wallet. And I share a little bit like what was the original proposal basically would require banks to apply very enhanced recordkeeping, verification, reporting any transaction involving mixing service. I'm talking about any, yeah, and it defined like mixing so broad that it covered pulling funds, cleating transfers, single-use wallets, asset swaps. You know, even when I was reading it, it was also about user-initiated delays. Yes, you may ask me, Alireza, or even delays. Even waiting counted, yeah, in that proposal and I believe withdrawing was a much better approach and since and still says criminals use mixers. So, this isn't a free pass. But back to your question, is Tornado Cash bad? People say yeah, Tornado Cash is a money laundering tool, I disagree. To my opinion, it is a neutral tool that enables privacy, not crime. To me it's like internet or Tor. Its existent allows, yeah, both legal and illegal use. But yes, you're right. You already highlighted as well that it was used for crime. But I would like to be honest about the numbers. When people talk about you know bring both statements, I like to see the statistics as well. With Tornado specifically its highs, its peak. The monthly inflows was around 400 to 550 million US dollar and illicit funds were accounted for 30 to 40 percent of that activity. So, the peak was in mid 2022, it was driven by major cyber-attacks, including Ronin bridge hack and yes, as you'll highlighted, North Korean hackers used Tornado Cash as well, but just be honest criminals misuse everything. They misuse cash, they misuse E-Mail, VPN. So, let's go back to numbers. 30 to 40 percent illicit also means 60 to 70 percent was not illicit. And then came the sanctions but imposed by OFAC in August 2022. So, one other question I have here also for the listeners for you also, Alireza, here. My question is are sanctions

even effective as a mechanism in a decentralized ecosystem because you know I have the data and it shows a clear limit. Both after the sanction era, the legitimate and illegitimate activity both drops by the use of Tornado Cash, but, and there is always a but. Actors still made a bigger share of what was left and then sanctions were listed and removed, legitimate users came back quickly. So, I mean, even US court that unconcluded a sanctioning immutable code, the way to sanction a person, you know, won't work. Basically, sanctions scare away the customers who follow the rules. Criminals don't follow the rules. The ones who didn't follow the rules stayed because they don't care about sanctions. So yeah, and as you mentioned, the other question is, are there legitimate uses of mixing services? Privacy protocols you highlighted very well about, you know, a charitable donation. Yes, there are many use. Personal financial privacy, maybe salaries are paid, medical reimbursement can be paid. An activist under a authoretarian regime may receive, you know, financial support from certain campaigns. We have anonymous charitable givings you give example of the war in Ukraine. We have, you know, private governance voting on specific proposals, but we don't want to have a social pressure. So, there are also legitimate use of privacy protocols. Some people would say but we need to stop crime. Of course, we need, we should,100 percent, but we have to look at the bigger picture and if we talk about statistics because they are the fact, UNODC estimated when I was reading in the information that 800 billion to two trillion US dollar is laundered globally each year and this is mostly through traditional financial systems. This is the UNODC code and Chainalysis also estimated crypto-laundering has reached at least around 82 billion US dollar in 2025. This is a fast growing slice. Yeah, it's largely by stablecoins, cross-border networks. But again, let's compare the numbers. We're talking about 800 billion US dollar to two trillion US dollar laundering each year. And we're talking about 82 billion. It's a big number. I don't underestimate it, but in a big picture, crypto is playing a still a smaller role. My question back to you, maybe Alireza, you asked me if Tornado Cash is bad, I gave my answer. My question to you is: Are banks bad? What do you think about that?

Alireza Siadat: That's a very good point. I mean I like your insights and I like the way how you challenge the things because you have experienced from all the sides. I'm absolutely with you and I would say no, Tornado Cash is not bad, banks are not bad. In end of the day it's the users and absolutely with you. Sanctions have, in my opinion, never the right effect, as you clearly said. If you sanctioned some person who selling weapons, but you can still buy the weapon, those who buy the weapon they’re criminals, they go and buy the weapon, those who would buy the weapon for a good reason because they want to protect themself or the police force or whatever, they would not buy it anymore. But still bad people would buy it. I mean when it was back in a day with Tornado Cash, I was shocked. You know in the US, you can publish public source a manual how to print if the 3D printer a weapon and then use this weapon and kill someone. And this is covered by the freedom of whatever, but you're not allowed to draft the protocol of mixer, Tornado Cash, a mixer because this is what Alexey did. He drafted a protocol, where this mixer can be used by different people for anonymous transactions. And in the end of the day, you got someone who wrote the source, but who is not in charge of how you use the source. And this is something which is in my opinion terribly wrong, but yeah, I mean, I like your point. And to close up this podcast, I

would ask you one final question because I don't want this podcast to end with a sad ending. How do you see the crypto environment going in respect to maybe compliance AML but in general? How do you see the outlook with crypto in general and also crypto compliance?

Hedi Navazan: On the Tornado, I just want to say something about privacy and you know if privacy is suspicious, then every curtain in your house is a confession. Yeah, so I think that's where I think privacy is not inherently suspicious and it's a foundation for free societies and where we are right now heading. I think crypto AML isn't about fewer rules. I just want to be very clear about it. We do need to have rules. We need to protect consumers, and this is a must-have, but it's about smarter rules. Yeah, it's about built for the technology we actually have. Yeah, we talked about blockchain analytics, evidence is important. I keep on emphasizing evidence over labels proportionately over panic and privacy is not a crime. So, if you remember just one thing from today, don't fear the blockchain. Learn how it works because good compliance, shouldn't feel the innovation, it should make it safer to build.

Alireza Siadat: Thank you. These are nice last words for ending this nice podcast. I'd like to thank you and also the listeners for today's podcast. Yeah, and we're gonna see us hopefully soon again, Hedi.

Hedi Navazan: Thank you very much Alireza for having me. It was a pleasure.

