Steptoe

Episode 229: Blockchain Takes Over The Cyberlaw Podcast

Alan Cohn: [00:00:03] Welcome to Episode 229 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. Thanks for joining us. We're lawyers talking about technology, security, privacy, and government. As you can hear, Stewart Baker has the week off, and it is another week of blockchain taking over the podcast. I'm Alan Cohn, of counsel at Steptoe & Johnson and also the co-chair of our blockchain and cryptocurrency practice, and I'm joined by several of the practitioners from our practice group this week, along with a special guest interviewee. So first, to join us on the News Roundup: Maury Shenk, a consultant in our London office, an entrepreneur including his involvement in a number of blockchain-related companies; Charley Mills, partner in our DC office, focused on commodities regulation and activities before the Commodity Futures Trading Commission; attorneys Claire Blakey and Evan Abrams, who work with our group and are going to be talking about securities and anti-money laundering issues. And again, I'm Alan Cohn and guest hosting this week in Stewart's absence. We are also joined as our guest interviewee by Sarah Compani, an attorney for Bitfinex. Bitfinex is a full-featured spot trading platform for major digital assets and cryptocurrencies, including Bitcoin, Ethereum, EOS, Litecoin, Ripple, Neo, and a number of other major cryptocurrencies and crypto-tokens. Bitfinex also offers leverage margin trading through a peer-to-peer funding market and has a number of other features enabling cryptocurrency traders, purchasers, and sellers to take advantage of different aspects of this new asset class. So without further ado, let's jump into some of the news. And so what we want to do – there have been a number of different developments since our last episode of Blockchain Takes Over The Podcast, and so we thought we would start with some developments involving the Commodity Futures Trading Commission and some litigation that has taken place that's kind of helping to

clarify some of the jurisdictional boundaries in this area. So Charley, maybe you can tell us about the amusingly named Cabbage Tech.

Charles Mills: [00:02:39] Yes. The CFTC has been very active in the blockchain and cryptocurrency area for several years now. One of those areas is its enforcement program. And about 10 days ago, it had its first litigated success against defendants who were accused of defrauding customers in soliciting trading advice in cryptocurrency, including Bitcoin and others, and misappropriating customer funds.

Alan Cohn: [00:03:14] So the CFTC had gotten involved in the cryptocurrency space back in 2015 to start, right?

Charles Mills: [00:03:22] That's correct. In an original settlement against a company called Coin Flip, which was accused of being a platform for trading cryptocurrency options without being registered to do that with the CFTC, and in that case, that settlement the CFTC declared Bitcoin and other virtual currencies to be commodities, which is a fundamental need-to-do in order to have the Commodity Exchange Act applied to it and the CFTC's regulations. And so with that having them declared commodities, they've gone forward on a number of fronts, including registering a swap execution facility and a designated contract market to allow trading in swaps and futures contracts on Bitcoin. Then in the enforcement area, they've brought several cases mainly against companies that would generally be considered retail fraud, where like Cabbage Tech the allegation is that people – the defendants – are soliciting funds from the public to trade their funds in cryptocurrency or to give advice on trading and without being registered and doing it fraudulently.

Alan Cohn: [00:04:42] So what was Cabbage Tech doing?

Charles Mills: [00:04:44] Cabbage Tech was soliciting individuals – principally I think from around the country and one customer I know from the case was in Canada – asking them or soliciting them to send them money, and they would give them advice on trading that money in the cryptocurrency markets and also provide the ability to

exchange from one currency to another. And some of the advice, as the court opinion reads, was going to be discretionary, where they would take your money and trade Bitcoin for another currency. And what the court found after a full trial – although, it was a peculiar trial because the defendants did not appear, but the CFTC did appear and brought in witnesses, and the witnesses testified, and the court's opinion quotes from their testimony in substantial part, and the basic theme was: they sent the money, they never got any service, they never got their money back, and the defendants were not doing what they were offering to do in their solicitations.

Alan Cohn: [00:06:00] So but the crux of the case – or at least what makes the case so interesting – isn't really the fraud aspects. We've seen a lot of – we've seen fraud in this asset class that's you know unremarkable in the sense that all asset classes have fraud associated with them, and the enforcement agencies are getting good at rooting out the fraudulent activity. So what was that kind of the real insight that we got out of this?

Charles Mills: [00:06:26] The real insight, the most important thing from a legal perspective, is that the CFTC was applying its anti-fraud authority on what would be called spot-or-cash market transactions that had nothing to do with futures, swaps, or derivatives. And there is a question under the statute whether their power covers that activity, and they've claimed that it does. And this is a case where the court found that it did. The court also in an earlier opinion in March reinforced their – the CFTC's, the agency's – earlier finding that Bitcoin and other cryptocurrencies are commodities, and so this is an important facet because there is some debate about whether the Commission's authority reaches into the cash markets.

Alan Cohn: [00:07:15] So you have two things coming really out of this litigation from a jurisdictional perspective. Number one: a reaffirmation – or an affirmation – that the CFTC's position on virtual currencies – declaring them to be commodities under the Commodity Enforcement Act – is sound. The court supports that finding.

Charles Mills: [00:07:35] That's correct.

Alan Cohn: [00:07:36] And then, even though the CFTC may not have authority to regulate spot trading itself, the commission does have the authority to take action against fraud conducted in those spot markets and not simply in futures markets. Is that right?

Charles Mills: [00:07:59] That's exactly the case. Yes.

Alan Cohn: [00:08:01] So what do you think the impact, the upside of this is going to be? Where do you think the CFTC goes from here?

Charles Mills: [00:08:07] Well, I think it will encourage the CFTC to pursue these principles in the spot markets, which is important because the spot markets also underlay the futures that are trading and some of the pricing of the futures contracts look to the spot market. So they're a critical piece of how market pricing is done, and the CFTC has been concerned about its lack of jurisdiction to regulate those spot markets. This gives it clear authority to go into the spot markets where there's fraud or manipulation and prosecute it, which should be a deterrence to that sort of activity.

Alan Cohn: [00:08:53] And so of course we've seen the Securities and Exchange Commission, the SEC, indicating increasing interest in the spot market from a broker-dealer perspective to the extent that crypto-tokens may in fact be securities and therefore fall under the Securities Exchange Act of 1934. Do you think that this may indicate that the CFTC may have a clearer jurisdictional mandate or interest in cryptocurrency exchanges where the underlying assets may in fact not be securities but may still be commodities from the commission's viewpoint?

Charles Mills: [00:09:32] Yes. I think the CFTC has been very clear. They care about the cryptocurrency markets. They care about the cash markets. I think for the most part, they're not seeking to regulate them at this point, but they are very concerned about fraud on retail customers – or anyone – and then the tie that they have then to the derivatives trading and swaps and futures, which the pricing of which to some degree ties back into the cash markets.

Alan Cohn: [00:10:04] Great. Great. Well, very interesting. It will be interesting to see what happens now. Obviously when a regulator has this type of you know kind of jurisdictional victory in court, it can sometimes signal that there may be more active involvement in that area going forward. Alright. Well, we talked a bit about the Securities and Exchange Commission, the SEC, what they're doing in this space, and we started with their interests under the Securities Exchange Act. But they also have been active with their jurisdiction under the Securities Act of 1933 and in particular with some recent decisions relating to new proposals around exchange traded funds. So Claire, do you want to kind of tell us what what's going on there?

Claire Blakey: [00:10:51] Sure. So there's been a lot of activity this summer over at the SEC about Bitcoin basic exchange traded funds. The SEC has yet to approve a cryptocurrency-backed ETF, citing concerns about the lack of regulation of digital currency and its vulnerability to fraud and manipulation, but this issue is certainly not permanently settled. So I'll start with the timeline of the SEC's recent actions before turning to a more in-depth look at their reasoning.

Alan Cohn: [00:11:19] Yeah that's great because I know people hear lots of different things about what's going on in this space. So I think a basic kind of what's going on on the ETFs timeline would be useful.

Claire Blakey: [00:11:29] Great. So a couple of months ago in July the SEC denied Cameron and Tyler Winklevoss's proposed Bitcoin ETF.

Alan Cohn: [00:11:37] This is the Winklevoss Twins of Facebook fame.

Claire Blakey: [00:11:39] Of course. Yes. By a 3 to 1 vote. This was actually their second application to list and trade shares of their Bitcoin trust. They first submitted a proposal back in mid-2013 which was rejected by the SEC in March of 2017. So this fund would have held only Bitcoins as an asset and tracked the price of Bitcoin on the Gemini exchange.

Alan Cohn: [00:12:06] And the Gemini exchange is also owned by the Winklevoss Twins. Correct?

Claire Blakey: [00:12:09] That's right. Yeah. Then about two weeks ago, the SEC rejected applications for nine Bitcoin-based ETFs from three separate companies: ProShares, Direxion, and GraniteShares. But several days after its decision, the rejections were stayed pending review by the SEC commissioners.

Alan Cohn: [00:12:26] So is that new, the fact that the commissioners wanted to look at this question? Seems like it, right?

Claire Blakey: [00:12:31] Right.

Alan Cohn: [00:12:32] You know with the previous denials it's just kind of been a denial, but this was unusual because the commissioners kind of stepped in and said, "We want to review this."

Claire Blakey: [00:12:42] Exactly. That's right. Although I would add that it doesn't necessarily indicate that a reversal is likely, just that you know at least one of the commissioners were interested in taking this action and setting the process in motion.

Alan Cohn: [00:12:57] And this was this was Commissioner Hester Peirce, right, who requested the reconsideration, making her at least momentarily a hero to the cryptocurrency community? She was quick to point out that it wasn't necessarily her enamorment with the technology more than just concern about the way that the commission had made – the commission staff had made – the decision, right?

Claire Blakey: [00:13:21] Right. And she was also the commissioner [who] dissented from the Winklevoss decision.

Alan Cohn: [00:13:27] Right. Right. Right.

Claire Blakey: [00:13:29] So the last item I'll mention is that there is at least one other Bitcoin ETF proposal before the SEC. The CBOE wants to list and trade SolidX Bitcoin shares, and this fund's creators have sought to address the SEC's concerns by, for example, setting an estimated 200,000 share price in order to limit the fund's appeal to institutional investors. And so in early August, SEC staff delayed a decision on this proposal.

Alan Cohn: [00:14:00] Interesting. So it'll be really interesting to see you know whether this is kind of indications that the SEC is beginning to soften its view on ETFs or whether this is just more kind of bureaucratic machinations that's going to simply end us up in the same place.

Claire Blakey: [00:14:17] Right. So turning to the SEC's reasoning. This really comes down – all of these cases come down – to their concerns about preventing fraud and protecting investors. The Exchange Act Section 6(b)(5) requires that the rules of a national securities exchange be designed to prevent fraudulent and manipulative acts and practices and protect investors and the public interest. So with respect to the Winklevoss's proposal, in sum, the SEC found that they failed to establish that the various surveillance proposals of the BZX exchange were sufficient to protect investors from fraud. More specifically, they said that the price of Bitcoin could be manipulated through activity on Bitcoin trading venues. They rejected the claim by BZX that it could monitor the Gemini exchange for potential price manipulation and also rejected the Winklevoss's argument that Bitcoin spot markets are inherently resistant to manipulation due to the decentralized nature of blockchain technology.

Alan Cohn: [00:15:21] And so this is interesting. This has been this persistent challenge of you know regardless of what the proponents of ETFs submit, the commission seems to continue just to voice doubt about the stability of the underlying asset.

Claire Blakey: [00:15:39] Right. So as we mentioned, Commissioner Hester Peirce dissented in this case. She seemed to be concerned about the decision stifling innovation and argued that the proposal met the 6(b)(5) standard, saying also that her fellow commissioners focused too heavily on the shortcomings of the Bitcoin market and failed to properly consider the exchange's surveillance and fraud detection capabilities.

Alan Cohn: [00:16:08] You know that's interesting again, and so we'll have to see if you know kind of that perspective can win out over what just seems to be general skepticism about the technology and about the asset class.

Claire Blakey: [00:16:23] And then with respect to the commission's denial of – the more recent denial of – the nine Bitcoin-based ETFs, they really just relied on very similar reasoning as they did in their earlier rejections, mainly that there aren't enough protections against fraud and market manipulations of the underlying cryptocurrency products. And so in the case of the Direxion ETFs, for example, they said that the market for the underlying assets wasn't of sufficient size to ensure that prices weren't being manipulated on other exchanges.

Alan Cohn: [00:16:58] So it will be interesting to see. You know folks continue to try to craft exchange traded funds proposals with the hope that you know at some point the commission will allow these through. We will have to see whether the SEC in fact can get over their qualms about the asset class and perhaps evaluate the proposals on their face and begin to allow exchange traded funds to enter the market. Well, great. Thank you, Claire. Alright. So switching gears over to anti-money laundering and financial compliance issues. We had a couple of different things come up over the summer. First, an interesting speech by the head of the Financial Crimes Enforcement Network, right? Ken Blanco.

Evan Abrams: [00:17:51] Yes, that's right. And the speech was notable because the agency really has not said much of late about their approach to blockchain and cryptocurrency. The kind of foundational guidance is from 2013. Obviously the industry has changed pretty dramatically in terms of business models and in terms of the

technology. So companies have been struggling somewhat to kind of fit that older regulation and guidance with new business models and new technology. So the speech was closely watched in that regard.

Alan Cohn: [00:18:26] Interesting. And so Blanco said a couple of different things in there, some of them that were kind of expected and some of them that were a little unusual. So?

Evan Abrams: [00:18:37] Yes, that's right. To my reading, I think there's kind of four key takeaways. One which was somewhat expected was the director reiterated that ICOs, or initial coin offerings, are money transmitters, meaning they're a type of financial institution that's regulated by FinCEN. The agency had said that before, earlier this year in a letter to Senator Ron Wyden, so that was not particularly new but interesting to hear from the director. And of course this hasn't been said by the agency in kind of formal guidance or in regulation yet, so we really just have this letter and now the statement from the director.

Alan Cohn: [00:19:20] Yeah, and it'll be interesting to see how that gets effectuated, right? Because of course there's a question as to you know: What does that mean about who needs to conduct what? Can that be outsourced to third parties? If you are using a model where there is a foundation that governs the platform and a for-profit entity that does the engineering work, who in that constellation of entities is the money transmitters that is the financial institution that has to maintain the compliance program and have the compliance officer conduct the checks? And how robust does that need to be for this asset class?

Evan Abrams: [00:19:58] Yes, that's exactly right. There's still a lot of uncertainty with regard to the regulation of ICOs, and as you alluded to, then also just a question of generally are all ICOs regulated as money transmitters? On the security side of course is the question about the utility token. You have somewhat of a similar question on the AML side with regard to certain tokens that are really not meant to facilitate money transmission and whether or not those fall into certain exceptions within FinCEN's

regulations. So there's still a number of unanswered questions with respect to ICOs, even after we have the letter and now this speech from Director Blanco.

Alan Cohn: [00:20:43] Okay, so we have the ICO issue. What else did Blanco talk about?

Evan Abrams: [00:20:47] So one thing he mentioned that is going to be of interest to a lot of people who are regulated by FinCEN is an aggressive approach to Bank Secrecy Act, or BSA, examinations. The Bank Secrecy Act is the statute underlying most of the anti-money laundering compliance obligations for regulated financial institutions. The director said, "We have over 30% of registered virtual currency exchanges and administrators that have been examined by FinCEN and by the IRS Small Business Administration," which is their delegated examiner, "and it's the goal the agency to ensure that cryptocurrency exchanges administrators undergo regular routine examination." And those are pretty intrusive and expansive examinations. They involve usually an on-site visit from people from FinCEN and the IRS. They involve a review of the compliance program and related documents and even a review of raw data related to exchange transactions or related to transactions connected to the issuance of a token. So they're pretty intrusive, and companies who might be examined in the future are going to want to think about whether or not their compliance program is up to par in light of that kind of aggressive approach from the agency.

Alan Cohn: [00:22:06] Interesting. So really pretty much any cryptocurrency exchange operator should be thinking very closely about their anti-money laundering compliance programs and what they need to do to ensure that they're complying with FinCEN regulations.

Evan Abrams: [00:22:20] That's right. Exchangers and also, as we were just discussing, what the agency calls "administrators," but what might more commonly be referred to as issuer of a token, an ICO, and so forth.

Alan Cohn: [00:22:31] Great. Okay. So we have the inspection piece.

Evan Abrams: [00:22:36] Yes.

Alan Cohn: [00:22:36] Then we get some weird stuff that's a little odder, right?

Evan Abrams: [00:22:40] That's right. The director in a number of instances in the speech referred to individual peer-to-peer exchangers and businesses engaged in peer-to-peer exchange and suggested that they had FinCEN compliance obligations. But this may raise more questions than it provides answers to. First of all, just what are the AML compliance obligations, but then probably more interesting: What is an individual peer-to-peer exchanger or a business engaged in peer-to-peer exchange? There's a lot of popularity right now around decentralized exchanges. There's also kind of the older model of a centralized but non-custodial exchange. And there has been fairly persistent questions as to how FinCEN regulations apply to those entities. I don't think this speech necessarily is going to answer those questions. It's probably going to raise more questions. But it is something to consider in reading the tea leaves with how FinCEN is going to approach those type of exchange models going forward.

Alan Cohn: [00:23:50] Yeah, so it's interesting. These are very different exchange models, right? A centralized but non-custodial exchange is something that many of the exchanges, that are brand names that people recognize, this is the way that they operate. There's a company that operates an exchange platform, individuals on board onto that platform, and then they engage in either buying or selling different types of cryptocurrencies from other people on the platform with the platform taking a small percentage of the transaction. You know that's a pretty well-known model, and for the most part, at least at the federal level, it's pretty well understood what the compliance obligations are, though at the state level it can vary. Decentralized exchanges is a much – it's a newer model and a much more open question about you know what in fact is the compliance model that applies to a decentralized exchange.

Evan Abrams: [00:24:46] Yeah, that's right. The non-custodial exchanges have for the most part, at least the larger name brand ones, opted to comply with FinCEN

regulations. I think there are some people, some commentators, out there who have question whether or not the underlying statute and regulations really give the agency authority to regulate those type of non-custodial exchanges. But for the most part they have adopted FinCEN AML compliance programs. The real question as you alluded to is going to be these decentralized exchanges, and that at this point is still pretty up in the air.

Alan Cohn: [00:25:20] Yeah. Interesting. And so what about anything else that Blanco mentioned in this speech that kind of you know folks should be thinking about or aware of?

Evan Abrams: [00:25:29] One final point that's somewhat interesting. The director noted that he's going to be leading a special forum of financial intelligence units from different countries around the world that's going to be focused on cryptocurrency. A little bit unclear what's going to come out of that at this point, but something to keep an eye on. You know if it leads to kind of increased harmonization and cooperation, that would certainly be welcomed by the industry. Of course it could also lead to more cross-border enforcement actions, which might be less-welcomed by some industry players, so we'll have to see how that plays out.

Alan Cohn: [00:26:04] Right. And it's interesting to contrast this area to the securities regulation area or the financial asset regulation area where there is wide disparities between the way that international regulators have approached this issue. We've seen a little bit more consistency from the financial intelligence units. And so an interesting reference that we might see even more collaboration and cooperation across international borders around these issues.

Evan Abrams: [00:26:32] That's right. And because you have the Financial Action Task Force, or FATF, which is kind of the international standard setting body with respect to AML that basically all major financial jurisdictions have domestic statutes and regulations to comply with. There is a little bit more overlap with regard to the different

regimes and various jurisdictions around the world. Of course there are still pretty important and substantial differences in some instances.

Alan Cohn: [00:26:58] Yeah, no, very interesting. Okay, and then briefly we also had the office of the Comptroller of the Currency popping their head back up in this area as well, right?

Evan Abrams: [00:27:06] Yes, that's right. So the OCC came out last month [and] said they were going to start accepting licenses for special-purpose national banks for FinTech companies. There [are] some open questions here on the blockchain side, especially with regard to what type of blockchain entities will actually be able to qualify for this license. The license is really due to the OCC's mandate for companies engaging in core banking activities. So with regard to this FinTech license for companies engaging in either lending or check paying. But of course because it's focused on FinTech, it's going to be focused on kind of the modern technological equivalents of those activities. And kind of how broad that is, which blockchain and cryptocurrency entities are going to be able to fit within that license has yet to be determined. But it potentially is a big advantage for some entities who will be able to fit within it because if you do get one of those licenses, there is federal preemption for many state licenses that you might otherwise need. So right now you have a lot of folks who are operating exchanges or issuing tokens or so forth who have to go around and get 48 different state licenses, which is a particularly difficult, cumbersome, and expensive venture. So obviously if you have the ability to get one national license, that would be considerably preferable.

Alan Cohn: [00:28:41] But the OCC has kind of tried to get into this space before, and they faced some pretty stiff resistance from the states. Do you think that we'll see that here as well?

Evan Abrams: [00:28:50] Yes. There was a lawsuit brought by state regulators initially when the OCC announced they were thinking about doing this. It was dismissed at the time because it was not actually final agency action when the suit was brought. Several

state regulators have come out and made statements that they oppose this new OCC license. So there's a possibility that that suit's going to be renewed and challenged in court, and we'll have to wait and see how that all shakes out.

Alan Cohn: [00:29:19] Great. Alright. Well very interesting. So and finally as our kind of roundup, let's turn internationally and ask Maury: Can you tell us a little bit about maybe what the EU finance ministers are looking at with respect to cryptocurrency regulation?

Maury Shenk: [00:29:40] Yeah, sure. So in the EU, while there's been regulatory action at the Member State level, particularly from tax authorities, the central authority, in particular the European Central Bank, hasn't done nearly as much as US authorities have along the lines of what we've been hearing today on the podcast. But there is a meeting of the EU finance ministers this week on Friday in Vienna, Austria. And there has been a leaked confidential note – or at least reports of what's in the confidential note – that they're planning to discuss challenges for digital assets, including money laundering and lack of transparency, which may be code for some of the financial issues, investor protection issues that we've been discussing, like those from the CFTC and SEC.

Alan Cohn: [00:30:35] Interesting. And so kind of what's your sense of where their direction might go on this?

Maury Shenk: [00:30:43] Yeah, I think that there will be increasing international regulation of all of these things. EU tends to be more regulatory than the US, but slower moving. So my guess is that you know it's been slower moving so far on cryptocurrency regulation, but that at some point that it will catch up. Particularly you know we've got extremely strict money laundering rules in Europe, including under the Fourth Anti-Money Laundering Directive that took effect about a year ago I believe. And I think that there will be a significant catch up in that area.

Alan Cohn: [00:31:24] It's been really interesting to see more as you say that the Europeans tend to take a more heavily regulatory approach, but yet they have seemed

to lag especially [at] the EU level, certainly in the anti-money laundering area. And also at the asset regulation area they have tended to – it's been some of the national regulators that have gotten out in front and ESMA has been slower to issue kind of more specific guidance and has done more kind of broad, general statements. So it will be interesting to see as the Europeans really try to catch up. There's also this European Blockchain Partnership. Can you tell us a bit about that?

Maury Shenk: [00:32:06] Yeah, so that's an intergovernmental agreement that was signed in April. I think 23 European countries, most of them EU Member States, but not all. So it's broader than just the EU, and it's basically an agreement to promote blockchain for public services, although it has broader scope than that. To follow on from the EU Blockchain Observatory which is more research focus, associated with over €300 million of EU funding for blockchain projects. This one, by this month, the signatories are supposed to agree [to] a list of cross-border public services that could benefit from blockchain and other use cases and then by the end of the year start to come up with technical specifications. You know this is an example of the EU being regulatory because this kind of stuff is left more to private industry in the US, but the EU wants to make itself a leading place for blockchain by central action. That hasn't worked very well in the technology sector in general, and I doubt it will work great here, but that is the EU approach.

Alan Cohn: [00:33:21] Yes. It will be interesting to see whether the EU is actually able to kind of stimulate entrepreneurialism through quasi-regulatory mechanisms or whether the kind of a more hands-off approach will prevail. The Europeans have definitely stated a preference as you said to be leaders in the use of this technology, and it is interesting the government does have a number of levers by which they can encourage the use of the technology and the development and piloting. It'd be interesting to see if this type of a governmental approach will lead to that kind of innovation.

Maury Shenk: [00:34:02] Yes. Time will tell. And Stewart Baker will have some choice words about whatever they try here in Europe.

Alan Cohn: [00:34:09] As he does about most anything that the Europeans do at a minimum! So yes.

Maury Shenk: [00:34:16] Yes.

Alan Cohn: [00:34:16] Alright. Well good. Well, I think that's a good snapshot of some of the news that's taken place since our last Blockchain Takes Over The Podcast episode. So I think this may be a good time for us to turn to our guest speaker and to talk a bit about some issues, specifically involving cryptocurrency exchanges. So Sarah Compani, attorney for Bitfinex. Thank you very much for joining us. And maybe you can just start by telling us a bit about Bitfinex and the trading platform, Bitfinex's trading platform.

Sarah Compani: [00:34:57] Thank you for inviting me. Bitfinex was founded in 2012 and was one of the first professional platforms. Therefore it had time to develop very advanced features, especially security-wise, given their history. It has now invaluable experience in this space and has built upon it, so I think it's a good opportunity to discuss the security features on centralized exchanges because, as Evan mentioned earlier, there are two types of exchanges today mainly on the market. There are centralized ones and decentralized ones. There are many aspects that makes an exchange being decentralized or centralized, but to simplify: when you speak about a decentralized exchange, what you mean really is that the custody of funds remain in the hands of the user. The problem today is that mainly on decentralized exchanges it's less convenient and there's less liquidity, so people are still oriented toward centralized exchanges, although as we can see it would not make sense in terms of security to store their private keys on a centralized exchange.

Alan Cohn: [00:36:16] Yeah. No. I think that's right. And of course we – I think for the most part the broader user, the broader kind of population, might be more familiar with the centralized exchange approach. And there have been a number of security challenges to that approach, everything from some well-reported hacks to concerns about SMS spoofing and SIM card hacking to thefts of private keys or other things of

people just simply forgetting or misplacing passwords. You know as an exchange that's had a lot of track record in this space, as you said as one of the earliest exchanges, you know how are you all approaching this question of security and some of the best practices for security by exchanges?

Sarah Compani: [00:37:10] So you're right. The hack greatly influenced the company's culture and management. To be honest, I learned a lot just working with them because all decisions include a security-oriented aspect. I like to think securing your account on a centralized exchange is just like securing your home, with the exception instead of holding your home keys, a gatekeeper holds them from you. So let me clarify. Although you are legally the owner of your house, you cannot enter your house without the gatekeeper. It's the same here. You own the funds in exchange – hot wallet or cold wallet – but you need the exchange if you want to withdraw the funds. So now imagine that you store very precious items in your house. It's not enough to simply lock the door. There are a thousand security measures that you can take to secure these valuable items. So the first question one should really ask themselves is: Why would you keep valuable items in your house, especially when the keys are held by a third party? It's risky, and it doesn't make sense. Why would you store digital assets in a centralized exchange when you could store them locally and secretly in, for example, a hardware wallet? This is the first question anyone who wishes to open an account on an exchange should ask themselves. If you don't need to trade, if you don't need to use the services offered on the exchange, don't put your money on that centralized exchange. It doesn't make sense. If you do need to use the exchange, think about diversifying them. Open an account on different exchanges and only leave the assets on the period of time that you really need to. Then if you want, I can go through various features of how to secure all this. This is really the fundamental you need to understand before even putting your money on an exchange.

Alan Cohn: [00:39:04] Yeah, no. Those are really good points, and they're not ones that are often kind of highlighted for folks when they think about entering this space, which is of course you have options for how you store your private keys. And as you mentioned, a centralized exchange essentially holds those funds for you, but you have

other options. A hardware wallet is essentially as you said a piece of hardware – almost you know there are many that look like a specialized USB stick – where you can keep your keys yourself. You can also even print them out and keep them in a paper form. So that first question of whether you really need the functionality of the exchange platform and if you don't whether you would be better holding your keys yourself is a really important question for people to consider. Now of course, once you've made that decision, then there are security considerations and security considerations that exchanges take as well that are useful to think about.

Sarah Compani: [00:40:10] Yes. So what users really need to understand is obviously – it's a great decision to choose which exchange you will use to trade because the security features of the exchange really matters – but the point of vulnerability today is the user itself. So let's say you are a little bit chatty or sometimes you like to brag about how much money you make. You post photos on Instagram, Facebook, Twitter, Telegram, [unintelligible], and by doing this, you are giving clues – not in a single day, like every once in a while – to a malicious third party. You are disclosing the fact that you own valuable items. Well, if you come back to the analogy, they still don't know where your address is, so they know that you have those valuable items, but they don't know where they are. This is why you should never reveal your personal address (i.e., never tell on which exchange you trade). And you should never leave clues on social media, enabling to associate your public key to your individual name. That means don't click on emails with insecure links. Never reveal information about your account on the phone. Customer support will never call you randomly to ask about additional personal information. Unfortunately, there are still customers falling for that. Keep your passwords and account information secret at all times. However, in practice hacks can be of course more elaborate. What happened recently instead of typing Bitfinex in the URL, customers can make a little typo so the domain name looks very similar and the Web page they land on looks identical to the home page of the exchange. But once you enter the credentials to log in, it doesn't work and it's already too late. You just posted your password and usually on a hack attacker's server. Thankfully there are many features, especially on Bitfinex, that you can use to avoid – even if you gave your password and username to someone else – to avoid having your funds stolen. And

physical good individual security practices – and you can go on the FAQ of Bitfinex. They are all detailed. But I'll give you a few of them. So the first thing that you can do – and for me really it's the basics – is to either enable a 2FA or use U2F. So 2FA means two-factor authentication. It's a software-generated one-time passcode that expires after a few seconds, and you need it to access your account. So the 2FA comes either on your computer or on your mobile phone, and once you have it set up, even if they have your password and username, unless they also steal your computer or steal your mobile phone, they cannot access your account. Then the U2F is simply a USB stick. So it could be for example a hardware wallet. And without that USB stick plugged into your computer, they cannot access your account. And what it does it also encrypts all information, so even if there's a malicious software running on your computer, because there is this USB stick, then no one can read what you're typing. This is really the basics. There are more advanced features on the platform for people who are really, really security-oriented. It's called IP whitelisting or detect IP address change. So you give Bitfinex your static IP, and whenever someone else has your password, has stolen your mobile device, has stolen your computer, has stolen everything they could, they could still not access your account unless they're logging in from the exact same computer having the exact same IP than you on the account. And if the IP address has been changed and you didn't whitelist the IP, but you said this IP is the only one which can withdraw funds, if you log into your account with another IP, then the withdrawals are locked. So since by default Bitfinex sends emails every time you log into your account, if someone other than you has logged into your account, not only your funds are locked, but any time you can just contact customer support and tell them, "Just lock account. It's not me. It's been hacked." And then we will freeze the account until we can be certain that the person we're talking to is the real owner of the account.

Alan Cohn: [00:44:36] What strikes me you know and what's been striking in hearing about some of the more recent hacks in the cryptocurrency community and also the steps that exchanges like Bitfinex are taking, both with respect to customer awareness and also some of the internal security steps that are being taken, is that a lot of this should sound very, very familiar [to] long-time listeners of this podcast because you see the cryptocurrency world, particularly the exchange world, really converging with some

of the best practices around cybersecurity generally. And it's been an interesting evolution for an industry that maybe a couple of years ago was seen as somewhat removed from mainstream cybersecurity issues and the types of issues and topics that we might discuss here to one where the industry is both grappling with the same types of issues that the broader cybersecurity community is grappling with and arriving at many of the same kinds of solutions. So [it's] been a very interesting evolution to watch.

Sarah Compani: [00:45:46] Well, to be honest, as a lawyer I'm pretty happy to see this because, especially in Europe, we have this new regulation GDPR everyone talks about. Really having clients that ensure privacy of customers' data is not only a good experience for lawyers who need to learn themselves how to protect these data and what happens when there is a leak, but it's also – the whole community benefits from these best practices coming along, both customers [and] the whole ecosystem.

Alan Cohn: [00:46:22] No, I think that's right. I think that's right. So moving away from security, per se, Sarah, what do you see as kind of the future for exchanges? What do you see as some of the major issues that exchanges are going to be confronting going forward and some of the steps that you think that they'll be contributing to?

Sarah Compani: [00:46:44] Do you mean in terms of legal challenges or challenges in general?

Alan Cohn: [00:46:48] Well, I think that it could be legal challenges from a compliance perspective, from a question of token listing standards, or more broadly things like accounting standards and others.

Sarah Compani: [00:47:03] Yes, definitely. There are two types of challenges. The first one is that all the questions that exchanges face are cross-borders issues. There is no one set of regulations that applies to us, and you really need to understand the various laws and how they work. Certainly one of the other types of challenge is when the regulation doesn't exist at all. And in this situation, not only you need to think about inventive or creative ways of solving the issue, but also you need to pave the way and

anticipate how regulators will later on deal with this topic. So it's really about predicting the future. It's as easy as this. The three major points that exchanges will face coming forward is probably fixing standards regarding the listing of tokens. So probably [the] most important aspects are customer protection-oriented ones [that] require audits for smart contracts, tracking ICO funds, the strength of the project or the team, the token's nature and functionality, compliance measures that were taken during the ICO. Who worked on the project, etc.? Then compliance-wise, rules applicable to [the] fiat world are not well suited for the crypto industry because there are many specificities attached to digital assets because, let's say, they are programmable, because their price is volatile due to the absence of metrics. Exchanges help define such metrics. But a holistic approach is expected by the ecosystem. And it is widely connected to the next type of problem, which is accounting standards: how to factor those digital assets in a balance sheet or simply a corporate accounting system. On Bitfinex you can make passive income by margin trading, or you can make interest by holding certain types of tokens. Or, even as I was mentioning, decentralized exchanges now offer sometimes a feature where if you hold a token, then you can also benefit from the whole value generated by the exchange itself. So how do you deal with this specific type of assets? And I don't even mention the hard forks, the airdrops, all these things that create their own subcategories of difficulties for accountants. Yep, there are many challenges coming forward.

Alan Cohn: [00:49:32] So what do you see as some of the places where the compliance rules that are applied in the fiat world are going to have to either evolve or where new standards are going to need to be developed for the crypto world?

Sarah Compani: [00:49:48] So I think I will go along with the question of metrics and in cases where we have a threshold, for example for reporting or for monitoring. It's not easy to put a threshold as a single number because the prices are so volatile that a same operation today will maybe reach a threshold tomorrow while the consumer even has not traded, but just because he held the token in his account and the value suddenly went up, then suddenly the threshold is met for the same type of transaction. So that really doesn't make sense. It should be more about patterns and behavior. Is a

behavior normal? Is a trading pattern something expected? It's a tough question. Certainly the banking sector and exchanges will need to cooperate together more because it's about the bridge of getting outside the fiat world to come into the crypto world or getting out or cash out from the exchange to go into the fiat world. This is really where people will need to work together in [unintelligible] the compliance rules.

Alan Cohn: [00:51:02] Yeah, it's interesting, and we've talked about on previous episodes where we've talked about blockchain issues how in the US you have securities regulators looking at tokens as assets or securities. You have FinCEN, as we talked about, looking at them as currencies. Or, as we talked about on this podcast, agencies like CFTC looking at crypto assets through the lens of their own jurisdiction, where in Europe, particularly in Switzerland, you have, for example, the financial regulator there you know creating kind of new subcategories in which to view these assets. So you have payment tokens which are like cryptocurrencies. You have asset tokens, which would be securities or derivatives, debt instruments, but you also have utility tokens, as Evan noted, where they will be formally recognized as a category of asset. What seems to need to now follow kind of along the lines of, Sarah what you're suggesting, is then well if there are new categories or subcategories of assets, then we may need new ways that we think about either regulating those assets or providing kind of prudential supervision or oversight to those types or categories of assets. And this will be an interesting area as regulators become more comfortable with you know how existing regulations apply to crypto assets. They'll soon reach kind of the point that you've suggested of the limitations of those analogies and where they will need to start thinking of new or different or specially designed ways of regulating or overseeing crypto assets. So that's really interesting, and I really appreciate the insight on that. We do typically, for folks who come onto the podcast, we give you the opportunity to talk about any kind of upcoming speaking events that you may have or that, in this instance, any conferences or major milestones that Bitfinex may have coming up. So anything you might like our listeners to know about or might want to highlight?

Sarah Compani: [00:53:18] Thank you. This is nice of you. Actually, Bitfinex holds a subsidiary called Ethfinex, so a decentralized exchange, and there is a governance

summit coming in September. People are very welcome to go look online about the details. It will be hosted in Lugano[, Switzerland], and we will be talking about the challenges of decentralization.

Alan Cohn: [00:53:45] Well, that's great. And that will be very interesting, and we'll very much look forward to the insights that come out of that. We really appreciate your joining us today on the podcast and sharing some insights about some of the challenges that exchanges face. Alright. Thank you again to Sarah Compani, and thank you to Maury Shenk, to Charles Mills, to Claire Blakey, and to Evan Abrams for joining me today. This has been Episode 229 of The Cyberlaw Podcast brought to you by Steptoe & Johnson. Don't forget: suggest a guest interviewee and we may send you a highly coveted Cyberlaw Podcast mug. Send your comments, questions, and suggestions to cyberlawpodcast@steptoe.com. Get involved on social media: @StewartBaker on Twitter, LinkedIn, and Facebook. And please, please, please rate the show and leave us a review on iTunes, on Google Play, etc. This helps new listeners find the podcast, and it also gives us valuable feedback. So we hope that you'll join us next time as we once again provide insights into the latest events in technology, security, privacy, and government.