Barefoot Innovation Podcast with Simon Taylor
Head of Strategy, Sardine & Co-Founder, 11:FS

***Note that transcripts may sometimes contain errors and that transcript timing notations do not match the posted podcast**

Jo Ann: I have been looking forward to today's show for a long time because I have the perfect guest for us for the moment that we're in and that is Simon Taylor with Sardine. Simon, welcome to the show.

Simon Taylor: Thanks for having me, Jo Ann. How are you?

Jo Ann: I'm doing great, and as I say, extra excited to have you with us today because we're recording this while the news about FTX is still unfolding, with more and more surprises every day, so by the time people listen to it, who knows how the facts may have further emerged. But we're going to spend some time talking about this crisis and pivotal moment in crypto and DeFi and get your take on it. And I want to commend to our listeners that they really need to read your newsletter, FinTech Food. I'll put the link in the show notes. And you've been posting in really thoughtful ways always, but in recent weeks, what is really going on with the FTX situation and what we need to do to maybe use this as a moment to make the financial system that we're in better rather than worse. So I want to start by just asking you to introduce yourself. Tell us your background. You're in the UK, you do lots of interesting things, so tell us about you.

Simon Taylor: Yeah, well, the abridged version is I actually left school at 16 to do computer science and got a job working for a British telecom. So I spent the first five years of my career as a software engineer, coding between mainframes and a website, which turns out to be a very useful thing if you ever enter financial services is to understand mainframes and legacy technology and how to modernize those. After sort of eight or nine years in telco, I then left and I got a job working for a company called TSYS. TSYS are an issuer processor, so they help power the credit card programs for companies like Capital One. I think at the time it was Bank of America. In the UK, it was Royal Bank of Scotland, and I had several jobs there. Initially I worked in the data center and then I was head of innovation there and my job was to come up with a new product, sell it to the first client, and hand it to a sales team.

So that was a wonderful education in the basics of computer science and the basics of FinTech and payments and a good grounding. In 2013, I started working for Barclays, initially again more on the payment side. So I got a lot of experience in both domestic and international payments types to add to the card payments experience. And then was asked by Derek White, the then chief digital officer to help him set up the innovation lab called Barclays Rise. And I was then asked by the chief technology officer to become the head of crypto R&D. And when you're head of crypto R&D at a bank, you get asked a lot by various regulators, various internal teams to come and explain this crypto stuff and this blockchain thing. And I did that for quite some time up until 2016. So a real tour of duty in financial services, everything from software engineering and delivery through to

selling to banks to working inside it and delivering with all of the various control teams and departments, right through now to where I sit today.

The last thing I'll mention is from 2016 through to about five or six months ago, I was also one of the founders of a boutique advisory firm in the UK called 11:FS. And again, there we worked with everybody from big tech firms wanting to get into FinTech and understand financial services to startups, to again, the very large, incumbent banks and financial institutions themselves wanting to become more digital and deliver better digital services. So I started blogging. Yeah, FinTech Brain Food is my personal blog. Please do check it out. And I try and bring that experience to an audience and I like to say that people tend to like it mostly because you can almost hear the British accent when you read it. So I hope that everybody enjoys it and I hope this is useful for the listeners and particularly those who are concerned about what FTX means and what crypto means and drawing on some of the experience I had, sort of hopefully trying to explain this stuff back in the days when I worked inside a bank. Hopefully, that's useful to your audience, Jo Ann.

Jo Ann: Fantastic. And before we move on, say what Sardine does.

Simon Taylor: Yes, of course. So I got a new job. I am the head of content and strategy over at Sardine. Sardine is the world's best fraud and compliance team that you hire as an API. What do I mean by that? Well, if I'm a FinTech company, there are a lot of activities I have to do in order to simply comply like being able to do KYC, have transaction monitoring in place, maybe having a great case management tool like Hummingbird, but often putting those together can be very difficult and indeed, you might tick all of the boxes on that stuff and still have a massive fraud problem.

And so Soups Ranjan, who was the founder of Sardine, had experienced both building a fraud and compliance team at Coinbase where he was between the world of DeFi and traditional finance and again, at Revolut. And having done that, he found that he had to integrate 15, 20 different vendors in order to get his fraud down without harming the consumer experience. And so he decided to leave that and spin out the infrastructure company. So Sardine is one contract, one API, primarily aimed at FinTech companies that can significantly reduce fraud. But what we've also seen is because we operate in high risk payment sectors like crypto, like e-gaming, and indeed around authorized push payments, we're now able to share that data with financial institutions to help them understand where the fraud risk might be emerging in these sectors, which I know a lot of financial institutions and indeed regulators are quite concerned about.

Jo Ann: Fantastic. So you have two real gifts I think that stand out in my mind. One is you have an amazing ability to explain these concepts to people who are not already deep in them. You're like a translator. As you know, I host a round table conference in the summer in Santa Fe, New Mexico, and this year I had you try

to explain DeFi to the non-crypto folks in the audience and gave you an extra platform because you're so good at doing that. And then secondly, you are so deeply insightful about understanding the big sweep of what is at stake and what's changing. And so I want to do both of these things with you, to talk about FTX. I actually had just met with Sam Bankman-Fried, it had to have been around the time that this whole thing was starting to break and I had the same reaction to him, but I think most everyone did.

I was very impressed and he was of course, making the rounds in Washington, as we know, talking with policy people and trying to put forward a constructive message for the industry on how to think through the policy challenges coming up. And we now, based on what we know today, are looking at what happened at FTX and there's a component of it that certainly appears to be about bad behavior and terrible or absent controls and the whole human side of failure. And then there's another set of issues around whether the crypto markets themselves are hopelessly flawed. And we're moving into a time when crypto critics are throwing mud really all over every part of the crypto and digital asset sector, hoping to get it all under control from a regulatory and legislative process. And certainly, we're going to have policy making all around the world. So I would just like you to share with our listeners how you're thinking about the lessons that we're learning from this case and the challenges we face and the directions that we should and should not go in as we work our way through it.

Simon Taylor: Fantastic questions.

Jo Ann: Yeah, it's not a small question.

Simon Taylor: Yeah, it's a lot to come through, but I think I heard three things, which is the human failure, how that impacts the entire industry, and what lessons we can learn. And I'll try and tack off each one of those. The human failure I think here is astonishing, but at the same time, very human in its nature. This does appear to be a case of drip, drip, drip over time if you look at the history that's available. And the shock is quite astonishing. As you say, many industry commentators could not believe this news when it came out. And I think part of that was because FTX had done such a good job at building its PR and reputation. The FTX Arena, Sam Bankman-Fried, the famous CEO, appearing on Bloomberg podcasts and live on TV, but also representing the industry on the hill.

That's deeply concerning for anybody who cares about this industry when there are clearly now findings of failures of the organization that individual represented. So is there a human failure with these things? Without question, but it's worth stepping through kind of what that was just ever so slightly, because there are two organizations implicated here. There's Alameda, which was a proprietary trading firm, and then there's FTX, which is an exchange venue. And what's happened between those two over time is there was a relationship between the two based on a new form of token called FTT. And essentially FTT functioned as sort of a loyalty reward point for users of the FTX

platform. If you have more of these reward points, if you have more FTT, then in time, your fees for trading would decrease and in isolation, there's nothing wrong with that. We've seen this many times before, that reward points result in lower fees.

You were encouraging behavior and activity. That intrinsically is not bad. And indeed the relationship between Alameda and FTX appeared to be above board on paper. But what happened subsequently is it turned out that their relationship was actually based on this token, on this FTT, because what would happen is the FTT token was entirely made up by FTX out of thin air, but Alameda would use that FTT token as collateral to take out loans and they would represent their balance sheet and ascribe a paper book value to the FTT tokens that they held and indeed, in some cases lent to or borrowed from FTX. And this is where things get difficult because the value of FTT token dramatically changed in crypto winter and this thing freely trades on public markets. It's 24/7, you can go see this stuff.

And a journalist found an example of the Alameda balance sheet, guy named Ian Allison who works at CoinDesk. And indeed, when the market on November 2nd started to see that, "Hang on a minute, most of this balance sheet at Alameda is made of FTT token, that's concerning. Let's get closer. Oh wow, they've actually lent a lot of this or there's a lot of lending back and forth with FTX. Does that mean FTX is safe and secure?" And that question led to a run on FTX. And the run on FTX then meant that very quickly a liquidity problem became a solvency problem and we had a run on the bank scenario. So what kind of failure is that? Well, it looks like a run on the bank on one hand and both of these businesses in isolation look probably okay, but then when you put this token in the middle of it, what that did is arguably obfuscate the relationship between those two organizations.

And that's not what the auditor saw, it's not what the market saw and that's the cause of the concern. And then the internal audits and controls that sit around that in a famously small company do appear to be somewhat limited. Now, I would say that this is all based on information that's been shared in the public domain. These are my personal views. I don't represent anybody involved in those comments, but I did blog about it at FinTech Brain Food and cite those sources. And we are now seeing that the new CEO of FTX has taken over and released some of this information. So that's point number one. Is this a human failure? Yes. But you could almost imagine how each of these decisions in isolation made sense by themselves. And then crypto winter suddenly made things a lot more concerning. And when you're a very small business that suddenly becomes worth $35 billion in what, three, four years, one of the most all-time high growth rates, where are your controls? Where is the risk management? Where's the experience for having done that?

Success hides many problems, unfortunately. And then when the market turns, it appears that sort of when the tide went out, there wasn't actually massive,

massive risk management there. Now some would argue if any organization suffered a run on them, they would need a lender of last resort, they would need some way to manage it. We nearly saw this in the global financial crisis. Crypto does not have an equivalent, but we can come onto the whole industry as I think a point number two. Is there a human failure? Yes.

But if you look at Bear Stearns and Barings Bank and all of these failures where, I think there was a Credit Suisse trader as well, these famous examples, each one of those where an individual trader may have gotten a bit too far, often it's them trying to trade their way back out of trouble that leads to this loosening these decisions. And it is very, very human. And unfortunately that is something that we keep learning throughout history. So is there a human failure? Yes. I've probably made many human failures in how I've articulated this to you. We are human, we do fail, but that and how it impacts the industry I think is worth talking more about.

Jo Ann: Okay, but let's turn then to what it is spotlighting about the design of crypto. In your FinTech Brain Food post for November 17, which we will link to in the show notes, you have a very thoughtful analysis of the role of trust in general and in financial systems specifically and what has been happening to trust with traditional finance and where we are with the inability to be trusting these crypto markets. I'd love for you to share this line of thinking with the listeners.

Simon Taylor: Absolutely. So trust is a word that we use an awful lot in financial services. And the problem with trust is it is one of those words where you say it too much, it starts to lose all of its meaning. But I went and looked at the human psychology of what does trust actually mean? And trust means to a person, "This thing I'm trying to do with this counterparty, this other brand, it's going to work. Not only that, it will work consistently." And thirdly, and the most important thing, it is dependable and if something goes wrong, I should be made whole. And the example I give is that whenever you see the Visa logo, it says, "Whenever you see this logo, the payment you're trying to make will work. It will work dependably and if something goes wrong, there are systems and processes to make you whole."

And that's often the case with the promise that banks always made. Banks always promised that, "We will lend to you but we'll do so responsibly unlike payday lenders. If you leave your money with us, we'll be here tomorrow and your money is insured by the government. This is the promise that we make." However, post-financial crisis, we saw a real vacuum of trust. Post-social media, we're seeing a vacuum of trust in mainstream media. People don't trust big tech anymore. People don't really trust the banks. If you read the Edelman Trust Barometer, consumers don't really trust anything. And almost as a reaction to that, you start to see the emergence of Bitcoin and trustlessness. In fact, in the very first Bitcoin transaction, we see the line, "Chancellor on the brink of second bailout," for banks quoted in January, 2009. Now I think in government and policy circles, they took this to mean that the crypto and the cryptography

movement was necessarily adversarial to the idea of good government and to the idea of trust.

And perhaps there are some people for whom that's true. However, like the internet itself, like a hammer, like fire, like the nails, there is simply no technology that is in its very essence adversarial to anything. It simply is. The question of the hammer is do you use it to build a house or do you use it as a weapon? The activity is often what matters as is the intent of the user. So when we think about trust, the promise we make from a CFI or traditional financial services world is, "We, the centralized intermediary, will make you whole. We, the centralized intermediary, will protect your identity and protect your data. We, the centralized intermediary, will be here forever." But people have started to question that. "What if the intermediary is implicated in FX, Libor rigging scandals, or mortgage mis-selling or has hidden fees and lots of charges?"

This gradually erodes the consumers' trust and brand perception over time. What if their services are hard to use? What if every time you call them, you have to deal with a robot instead of a person? This, again, erodes trust. Whenever traditional financial institutions see their customers as a cost and not an asset, they erode the trust of their users. There is a vacuum of trust. So decentralized technologies make a different promise. They say instead, "This technology is transparent, there is no middleman and you can see it all for yourself. The code is law." Now there are some problems with that promise. If you can't read code and software, then how can you tell what it does? Sure, but how can you tell what's going on inside of a financial institution? Do you read their internal audits? Probably not, but it is a different promise.

But the problem with this promise is it's not necessarily been held up. In fact, there was a good study by the Bank of International Settlements that suggests most consumers, between 75 to 80% of retail investors, have likely lost money on their investment. So if the promise we make is, "It's transparent, so it's better," if the promise we make is, "It's open, it's inclusive, there is no middleman, so it's better," have we materially improved the lives of consumers? I think the answer to that is not yet, but we could. And I think that's the lesson we need to learn is how do we do that. So I think we can get there, but there are lots of problems to solve.

Jo Ann: So talk more about that. In your paper, you talk about what's on-chain and what's not on-chain. If it's on-chain, it's transparent. And even if I can't read the code, I can know that lots of eyes are on these kinds of things or should be, but right now we have hybrid models where the transactions are transparent on-chain, but the business activities are not. What's your line of thinking on how we might be able to strengthen the trustability of these systems?

Simon Taylor: Yeah, I think this comes down to paper money versus the on-chain value exchange to your point. Anything that happens on-chain is a public record, which immediately begs a question... Sorry, it doesn't beg a question. It raises

the question. Sorry for being pedantic there. It raises the question about privacy and security and so on, but let's just set those aside for another day. If it happens on-chain, it is an axiomatic fact, "This thing happened and maths can prove it." Thousands of computers around the world can perform the same math and prove that this did in fact happen. But if somebody uses that transaction and takes a loan out against it and does that on a piece of paper, we have no way of knowing that that happened. So one of the things that you see is we get into this idea of self-hosted wallets versus custodial wallets.

So on-chain, I can self-host my assets, the equivalent of having cash in my pocket or cash in the mattress or carrying around a gold bar. I am in custody of that asset and I would have instant settlement as soon as I give that asset to somebody else. Just like giving you a bar of gold, you now have that thing and I no longer do. It works that way. And the way consensus works is if there's a room full of people, they can see that I gave you that bar of gold and you now have that bar of gold and I no longer do. That's consensus and that's instant settlement that happens with any on-chain activity. So that's self-hosted wallets. Custodial wallets come along and say, "Well, actually that is kind of difficult for a lot of people to do because the problem with being your own bank is you have to manage your own bank robbers. So we'll step in as a middleman and we'll protect you."

And so you see lots of good businesses like Coinbase and Kraken come along and attempt to do that for users. They create a better user experience, but what they'll do is they'll hold onto the funds on your behalf and give you a username and password. Now when those exchanges transact those assets, they don't necessarily have to do so directly on-chain. They could essentially have a pooled account in which all of those assets sit and be much more efficient in the process. And we've seen this in banking for many decades. We have sort of FBO accounts and many other structures that allow for that efficiency. But the problem is now I've lost my transparency of where my funds have gone. There was a great paper by Vitalik Buterin, the inventor of Ethereum, that talks about how you can actually have both privacy and see where your assets are.

But in a simple example, maybe I don't need to see exactly where my assets are, but I would really like to know that if I'm dealing with a centralized exchange, it is at least solvent. It is at least has those assets. It's not sent them somewhere else, it's not rehypothecating them. So what organizations like Kraken have done and now Binance are starting to do is prove their solvency on-chain by publishing their wallet addresses and publishing where those assets are. So now it is a matter of public record, which trading venue is solvent and we will still get into more complex issues around assets versus liabilities and privacy, there are lots of issues to solve there, but that transparency is an interesting premise because I think about the controls we had in the policy world and the regulatory world.

We were reliant on audits. We were reliant on reporting from the financial institution and actually in this case that wouldn't have solved anything. If the reporting from the financial institution is incorrect or in many cases misleading or just wrong, then regulators would not have been able to do anything to prevent this activity or see it coming in any form of enforcement. Whereas the on-chain transparency, any transaction that happens must be published and that is in the code, could be really powerful.

Jo Ann: So we know we can't always trust people and we know we can't always trust complex business systems or regulatory systems. So the dream, the question is whether we could trust the code, knowing that it's written by people and that there are still things that could go wrong, but you can potentially create a system where it's not just a statement that something's being done, but it's built into the technology itself. I'm going to circle back if we have time before we finish to maybe talk about the promise of DeFi, things that might be better if we could see the full flowering of some of these changes. By the way, I met Vitalik recently and invited him on the show, so I hope he's going to come. We'll see.

So we're in a moment where regulators and lawmakers, again, all over the world are looking at this issue. When you have something like the FTX controversy, it not only activates the people who were already paying attention to the space from a policy standpoint, but it also draws in a lot more people, politicians whose constituents are concerned or have been harmed but maybe don't have depths of knowledge in it. And again, regulators suddenly feeling like they need to do something. Let's start on the policy side with what you're worried about. What are you worried that policymakers may do in response to the FTX situation that would be a misstep or a mistake?

Simon Taylor: I think assuming that the answer is analog regulation and that would be effective. I'm a big believer in regulation when it's effective is the most important thing for consumers. Effectiveness matters. We could create massive cost, we could damage innovation and have no meaningful improvement in consumer outcomes or limit consumer harm in any way. So that activity just feels like an unfortunate waste of time. And if the only goal is to be seen to be doing something, then tick in a box. But if we're really here to prevent consumer harm and to be effective, then we should look at what would be most effective and sort of leaning into what the technology gives us and is capable of is important. I think I would be worried about that. I've seen lots of examples where actually often the policymakers and indeed some of the politicians are extremely well-informed in this space.

So I'm encouraged by that. Indeed, the audience listening to this are probably engaging with that subject for that reason. But you asked me the worry and I think that that would be worry number one. I think worry number two is that we throw the baby out with the bath water. I think the harm here will be extremely unfortunate and horrible, not only to the customers that have lost out but the potential contagion risk. There is real harm there, but I do think therefore we

can't assume everything in this category is bad. My frustration with the subject of crypto and particular DeFi is it is simultaneously the most sublime and the most horrific subject on earth in that you can get these horrible, horrible examples of North Korea hacking wallets and you can see organized crime activity, transparently I might add, and effectively enforced. And then on the other side, you see some of the brightest minds, some of the most interesting people doing things that could be genuinely transformational for the global economy.

Why do I think that? And I think we need to step back to the first principles here. This is a global, 24/7, financial infrastructure that is digital in nature. If you go look at the history of our financial services infrastructure, we started with a piece of paper or in fact we started with stones and then we got to precious metals and then we got to barter and then we got to beyond that into paper and then we got from that into blah blah blah. I won't do the history of money. But essentially it's always been an evolution and especially over the last hundred years and in particular, we see national systems that are globalized rather than truly global. And possibly the only example that we see that is really, really like crypto is the foreign exchange or the FX markets. And the FX markets don't neatly fit inside one single jurisdiction.

And so the problem we saw with FX is the jurisdictions might have had ironclad, world class rules about how FX should be managed and traded, but yet we saw the Libor rigging scandal and we saw many, many others. And it wasn't until there was a global code of conduct pushed by the central banks and the international agencies and the financial institutions themselves and the market participants that this was meaningfully impacted. And indeed, crypto is natively global. DeFi is natively global. It's natively 24/7. It could be much more efficient, it's natively programmable. We can bake the rules into in a given asset class or a given transaction, but who's rules? Under what jurisdiction? And I think that's particularly challenging because if you make your jurisdiction too tight, then you might remember that FTX was based in the Bahamas and there are many "offshore" crypto exchanges.

You have to find that balance and I think it's going to need global coordination. So you have to zoom out to actually what is this thing in front of me? What is this global 24/7 infrastructure and am I risking playing whack-a-mole and pushing all of the activity offshore here or do I need to work with this technology and legitimize it? So there's that problem. And meanwhile, FTX has this contagion risk. Uniswap, Aave, Compound, a lot of the stuff that is true DeFi continues to run without a hitch. It's absolutely fine. Everybody that's self-hosted their wallet is not implicated by FTX at all. So there's nuance and there's detail here. And because there's nuance and there's detail, the temptation to copy and paste what worked in traditional financial services just doesn't hold up.

There are good principles and the first principles of finance and good risk management absolutely apply. You should be solvent. You should be thinking about how you're accounting for that. Of course, we should, in first instinct, do no harm to consumers. We should treat customers fairly. We need segregation of customer funds, we need all of those lessons from history. But the way we implement them I think cannot assume existing way we implemented it in traditional financial services. We need to work with the technology, not against it.

Jo Ann: That is so well said. And also your point is very well taken. There are a lot of very, very sophisticated regulators and lawmakers looking at all of this now. And as you know, our show has a very high percentage of policymakers who follow it because we always pay attention to the regulatory issues. So let me ask you to circle back to the first point that you made about the risk of trying to regulate this with analog approaches because as you say, the principles are timeless. I mean this whole situation is going back to basics on the need for governance and the need for these principles that you were just listing. It's common sense, it doesn't change. But if you were a regulator today and you understood the concept of what you're saying, that analog regulation isn't going to work here or work well enough, can you take that down to another level of description and talk a little bit more about how regulators should go about creating a digital regulation of these inherently digital age financial services?

Simon Taylor: Yeah. Well, we should point out that there are examples where standing legislation and regulation already applies to the crypto industry, whether it's money transmission laws and their global equivalence. Whether it's anti-money laundering, KYC, AML, there are lots of rules that already apply and are already implemented. So that's point number one. But we see even in the anti-money laundering law enforcement circles, they are using the tools like Chainalysis and TRM Labs and the on-chain forensics to be much more effective in how not only do the exchanges report, but they share information with law enforcement. And that's one good example we could really build on. And so this space is still emerging. The problem I think for policy and regulated communities is we're trying to regulate the plane as we're flying it and it's being built at the same time.

So it's extremely difficult. So what I would propose is the use of labs and the use of co-regulation where the industry is able to identify best practices, where the industry is able to build solutions, we do so transparently with policy and regulators so that we can proactively say from a practitioner standpoint, "Here is where we think the issues are, but also here's something we're trying to meaningfully mitigate that risk and in aggregate, we'll learn from the whole industry and start to adopt those tools." So I think co-regulation is going to be extremely powerful to look at. And secondly, within that co-regulation, can we start to bake in different forms of reporting? I think the nature of reports existing as a PDF is kind of unfortunate for everybody.

Receiving a PDF and then trying to enforce on the back of it or even understand what the heck the thing says, I feel for everybody that works at an agency. That's no fun because really what you're dealing with is the standard that could be implemented by the worst financial institution so that they could comply rather than what's possible. Whereas the technology in crypto and DeFi is kind of out there, it's very, very modern. What could we report and how could you have instant visibility, instant oversight, early warning systems of risks before they build up? And what would that dashboard look like? What would that supervisory tech look like? I think is a really interesting question to think about. But what I don't know is what are the requirements for that? What do you need to see? What would you like to see? What I can help to answer is where the risks are from the practitioners. I should declare an interest. I'm a founder of an organization called Global Digital Finance, the division of the Global Blockchain Business Council.

And we built a set of codes of conduct and global best practices in the full view of the global regulatory bodies like the FSB, BIS, IOSCO, VAT-eFS, CPMI, and many, many others and their peers. And the reason we did it with those agencies was because we recognize that it's global and we should create a high watermark and that there are risks that are not captured by standing regulation that will emerge that we can manage today, but that this is a moving target, that there's not going to be one law that you pass that captures all of this. In two years time, something else is going to happen and in four years time, something else is going to happen. So what does that space look like? And I think that's where co-regulation becomes really, really powerful. We're not necessarily saying self-regulation, we're not saying, "Stay away from the existing agencies."

All of that has to continue to exist and will. But where there is this gray area, we can look at that. That would be my call to arms. The last point I'll leave you with is the MiCA legislation in Europe, I actually thought was very, very sensible. It uses the definition of self-hosted wallets. It materially expects so-called stable coins to be able to manage their solvency and to have good backing and segregation of customer funds. There's a lot of the principles we've talked about in this conversation that are baked into MiCA and Europe is not a superpower in many things these days, but I do think it's a regulatory superpower. We saw that GDPR kicks off a lot of the privacy conversations. We saw that PSD2 kicks off a lot of the open banking conversations.

I suspect we'll see similar lessons to be learned from MiCA. So if you are not from Europe and you've not paid attention to the MiCA legislation, I would definitely go pay a look at that. And I think there's a good example we can build on from that as a basis. And around that, can we think about co-regulation to move into supervisory tech, to move into the emerging issues, and to make that more of an ongoing conversation rather than one-off actions and one-off conversations.

Jo Ann: I couldn't agree more. One of the biggest challenges here is going to be to modernize the regulatory infrastructure and data and architecture, but then to change it continuously instead of every decade or whatever. That in itself is a huge change. So Simon, you've already answered a lot of this. Maybe you've already answered all of it, but I do want to take this back up to the top of the vantage point. And it's an unfair question to ask you to opine on this because I know no one has all the answers at this point. But what would be, that you haven't already covered, what are the main elements of an appropriate legislative and regulatory response to the moment that we're in? Are there things that you haven't said that you think policymakers need to pay attention to getting right?

Simon Taylor: I think the one thing I really want to see is recognition for the potential of the technology and not in that sort of, "We like digital assets, we don't like crypto," sort of bifurcation, but a recognition that a technology is a tool and that a technology is a tool that can be used for consumer harm and economic harm and market abuse, but it's a technology that could meaningfully create more efficient and orders of magnitude more transparent markets. And if we get this right, we can build a much, much more efficient and fair and inclusive global financial system. And that could be the next big thing in technology if we do get it right. It could be astonishingly impactful to the entire human species. So that is a difficult balance. I would not want to be the one that has to make that statement, having agonized over reports and published them out there.

But I think that recognition of moving away from digital assets, good, crypto, bad, and moving towards risks, bad, opportunity to manage risks with the technology and with principles, good. And that's an important nuance that I think at the most macro level we should really, really work hard to strive for. And we should recognize that some of the labels we use like DeFi that might be quite emotive, some of the labels we use like crypto that might be quite emotive are not necessarily bad. And that within those, there are useful tools that could improve outcomes for consumers, prevent market abuse, and prevent harm on a massive scale. So I think that would be the most important point that I'd want to make. And then I think the other point that I'd want to make is I'm not letting the industry off the hook here at all.

I actually think the industry has the most work to do to stand up and deal with the fact that there is a massive fraud problem inside the industry. And I would say that I work for a fraud prevention company, but at the same time it is. If you talk to any financial institution, the fraud coming from crypto is still way too high. The industry has to up its game. If you want to look at the scams and the hacks, still it targets the crypto industry and that has to be something we get better at. There is still too much market abuse, still too much wash trading. The industry must raise its game and it must do so transparently because the crazy thing about crypto is... I think we saw that some of the Mt. Gox victims have finally been repaid from 2013 in recent news.

Crypto is forever. On-chain crime gives law enforcement forever to figure out what's going on. So if we don't up our game, law enforcement will get to that caseload eventually, they will get there because unlike the world of traditional financial services where it's opaque and maybe you're trying to put together a spreadsheet in an email and a PDF, if it's on-chain, it's permanent and it's never going to go away. So the industry, you have an obligation to step it up. If we want to deliver this better financial services, this more efficient, fair, transparent market, you have a duty to step it up and engage with regulators, but do so on a basis of education, open hand, and know that there are limitations to working in an agency. You don't have unlimited budget, you don't have unlimited mandate from law to be able to do certain things, have empathy from who's across the table for you and I think we'll do a lot better.

Jo Ann: There's a quote from you that I like to use and I'm not going to remember it word for word, but in your FinTech Brain Food one time you said something like, "It's the wild west and you can kind of do what you want before the laws sort of catch up to where you are. But don't forget that everything you do, if you're in the crypto world, it's always going to be there." You said something like, "Be careful out there people because everything you're doing can be seen." I think it's something that people do forget sometimes.

Simon Taylor: Oh, absolutely. The guys at the Bankless podcast, which I think is a fantastic podcast-

Jo Ann: Yes.

Simon Taylor: Often talk about we're at the frontier. This is not for everybody. But the difference with the frontier during sort of the 1830s and the late 1700s was there was no permanent record. The crimes that happened, where was the evidence? If the sheriff showed up, A, how legitimate was the sheriff? But B, where was that permanent record? On-chain activity is forever. I would posit to you that Bitcoin would probably survive a nuclear war. It is incredibly hard to get rid of this stuff because so long as there's a full record somewhere running on some laptop, this thing will keep running. It is the opposite of the traditional security model where we build up one centralized tower extremely high to manage risk. It spreads that risk among as many computers as it can around the world. And so long as a few of them continue to operate, it will maintain the truth. And there's an economic incentive to maintain that truth. On crypto, it's forever. On-chain, it's forever. So yeah, be careful out there, folks.

Jo Ann: Cool. Is there anything that you want to add?

Simon Taylor: Yeah, I do think that, this has been kind of an unfortunate conversation, but we have an opportunity here. Whilst everybody else is concerned and worried about the market being down and kind of the technology being bad and dealing with the negativity and all of that, and rightfully so, I just want to hold out a candle for hope here. I just want to say that actually if we could get rid of some

of the demons that Crypto has, if we could meaningfully balance policy and the technology, I'm so excited for what we could build. I mean, it really does fuel me, the idea that we could have a meaningfully more efficient, fair, and transparent market. I really do believe that, from my years in this industry. So I'm excited to have this conversation with all of the listeners. I hope we get to meet all of the individual listeners at some point and we can build this together.

Jo Ann: Fantastic. And tell us where our listeners can find the newsletter, Sardine, anything else you want to point us to? We'll put it all in the show notes.

Simon Taylor: Yeah, you'll find me on LinkedIn @SimonTaylor. If you're a Twitter person, @SyTaylor. Search for FinTech Brain Food on Google and you'll find the blog. fintechbrainfood.com is another way to get there. You'll find Sardine, the world's best fraud team that you hire as an API, at sardine.ai. And we are actively seeking engagement with policy and regulatory communities to understand how we can support them as well. And I'm also affiliated with Global Digital Finance, which is a nonprofit and it produced some codes of conduct and you'll find that at gdf.io. So I would encourage everybody to check those out as well. And thank you so much, Jo Ann. I can't wait to hear this episode and many, many more to come.

Jo Ann: Me too. Thank you so much, Simon. That's Simon Taylor. Thanks for being our guest today.

Simon Taylor: Thank you.