Eric: So I'm really excited to bring you Elena Nadolinski, founder of Iron Fish and Craig Timm their general counsel. Now, Craig Timm's portion comes later in the episode because he, we had the episode with Elena and then OFAC put Tornado Cash smart contracts on their sanctions list, and we decided to do a follow up and that follow up overlapped with Craig Timm joining.

So we had that at the end of the episode. And what's really interesting about this episode is that Iron Fish, which is a project and startup mode building a privacy token for on chain private transactions. We had her on earlier and we talked a lot about her as an entrepreneur, what led to the decision to build Iron Fish. Some of those gut wrenching pivotal moments that define you as a leader and an entrepreneur that she has had to made over the last few months.

It was open honest discussion. I love those kinds of discussions, cuz you learn so much about a leader and the project and really the blood and guts and what makes these privacy coins tick? What are they really thinking about and what impacts their decisions. It's valuable if you're trying to build a project yourself and Elaine's very open about willing to share with entrepreneurs and people working on projects.

And it's just to me, it's fascinating and you learn so much about the space to hear what they go through, and then we also build into why privacy is so important in transactions and dispel the myth of that a right to privacy is somehow nefarious or not for the greater good in fact it's a very important part of the evolution of blockchains in the use of blockchains and transactions.

We are also it's really funny because we talked a lot about that. We talked even about Tornado Cash and the elliptic report that linked some of these illicit transactions to Tornado Cash. And then I even made a mistaken, but oddly prescient reference to the OFAC report that came out last October as referring to Tornado Cash.

It didn't, but I was just having a vision. I wasn't wrong. I was having a vision. So at any rate so we add that part with Craig Timm at the end of the episode where we also talked about this. And so what you get is this really interesting podcast that sort of evolves through the.

The pivotal decisions underpinning Iron Fish, talks about the importance of privacy and some of the regulatory issues that are being seen. And then you we add on this perspective in the post Tornado Cash smart contracts, I don't know what we call that, era, but the event. And we talk about that.

So what you end up with is a really intriguing, intricate mashup, although structured mashup of all these different issues and privacy token. So I think it's a phenomenal episode. I'm really excited to bring it to you. I think, if you're gonna listen to this episode, you should listen to it with an open mind.

You should listen to it with open ears. You should get yourself in that mental state where you can be present and listen to every part of it, because there's just so much here and you can learn a lot. And if you're not, you're not asking the right questions. You're not listening actively enough that I always say this with the podcast anyway, like I, I try to really lay things down in a much more,

it's nothing fluffy here. Everybody who listens to this is mentally engaging and benefiting. It's not just something you put on as background noise. So at any rate, and if you enjoy this podcast, share it with others. I love to see this being talked about on Twitter and social media when the podcast come out and listen listenership is just continuing to go up.

I think people are getting the word out and I think the show is getting a lot more interest. And it's wonderful. So please continue to press it. Cuz I think there's a lot of dialogue going on here. There's a lot of value that, that we present that it could be valuable to a number of people and that's really the central mission of what I do.

I don't even take a sponsor yet if you happen to notice by design. I don't know how long I'm gonna do that for, but anyway with all that said I welcome you to enjoy the show. And with that, I bring you Elena and Craig from Iron Fish.

Welcome to The Encrypted Economy, a weekly podcast featuring discussions exploring the business laws, regulation, security, and technologies relating to digital assets and data.

I am Eric Hess, founder of Hess Legal Counsel. I have spent decades representing regulated exchanges, broker dealers, investment advisors, and all matter of FinTech companies for all things touching electronic trading with a focus on new and developing technologies.

This is Eric Hess with The Encrypted Economy and on today's episode, I am so excited to have Elena Nadolinski, CEO and founder of Iron Fish on the podcast. Welcome Elena.

Elena: Thank you. So glad to be here.

Eric: Yeah. So glad to have you. Exciting, a lot to cover today and exciting podcast. But let's start off with your background cuz it's quite interesting.

Yeah. Gosh,

Elena: where do I even start? So I was originally born in Russia. My parents came over here when I was eight. They were both software engineers. That's actually how they're able to come to the United States and they did reverse engineer or reverse psychology on me. They basically said you don't wanna be software engineer go do something more exciting with your life.

And so they always had programming books filling up the bookshelves. So slowly, but surely I started getting interest and the inevitable happened. I chose computer science.

And so I first actually went to Microsoft is my full-time job after college realized I wanted to join the startup world and moved to Silicon Valley to join a company called Tilt.

Tilt unfortunately didn't make it as a startup, and so we were acquired by Airbnb. And while I was there 20 17 20 18 era, the entire city of San Francisco was talking about crypto . And so that was my introduction to even discovering crypto and the Ethereum community.

And I can go on from there, but that was my introduction to tech and crypto.

Eric: Excellent. We'll go a little deeper into it. I think you have some tidbits of people you met early on and ways that they inspired you and moved and shaped you to where you are now.

Elena: Yeah, so the way I discovered crypto was from a dinner. So I think it was mid-2017. I went to a dinner at Juan Bonnets house for labs used to live and work at the same house. And it was such an incredible environment. Everyone there was talking about Ethereum says, I think the price like went to 30 or something.

And I just remember Googling the way back of what, like what is Ethereum and reading tutorials about it. And I'll be honest. I didn't quite understand the significance of it at first. But I did decide to attend Eth Waterloo, which was the first Ethereum specific hackathon that Eth global sponsored at University of Waterloo.

And when I went there, I was just blown away at how open the community was. Obviously this is a very early space, but everyone there was just so accessible MakerDoa team was there Vitalik was there. Basically every single kind of early team was there. Dan Finlay who wrote Meta Mask or was a huge contributor to it.

He was there and he helped me with my project at 3:00 AM. So I was just amazed at how open and welcome the community was. And I knew right there that I wanted to be more involved with it.

Eric: Excellent. Excellent. And now becoming an entrepreneur. So what, so tell us a little bit about Iron Fish and what inspired you to go down this road?

Elena: Yeah, so actually that very first hackathon project and I went to many more hackathons. Went down to the path of NFTs, but the very first hackathon project was about decentralized video streaming. So the project itself was how do you take a video of a video file, chunk it up into as many smaller pieces, put it on IPFS, which is which is a decentralized video storage or file storage,

and how do you make that accessible in like a decentralized video streaming environment? So one thing that I realized is that even though Ethereum is marketing itself as this world

computer, it's not really a world computer in the sense that you can't exactly give it a video file to Transco.

That doesn't quite make sense. So I was really focused on how we create a network that has honest compute, meaning that if I give a server a complicated task to do transcoding a video how do I have a system such that if that server gives me an output, I know that the output is correct without redoing the computation myself.

And so I went to meetups in San Francisco. There were a couple projects working in the space. And so I met True Bit for instance, and I kept asking the question of, how do we have a system that has honest compute. And slowly but surely people led me to zero knowledge proofs. There was one person at a party at a happy hour, I think, I was talking to them, and they said, you should really read this Pinocchio paper, which was the found the foundation paper that led to Z Cash's sprout first algorithm for privacy transactions.

So that's how I discovered zero knowledge proofs. And when I decided to quit my job at Airbnb and join crypto full time I realized that privacy in particular was such a huge opportunity and a very huge gap in the ecosystem. So at the time, 20 18, 20 19 era many teams were working on how do we create stable coins?

How do we have higher throughput of transactions? But almost no one was working on privacy. Which to me was, such a huge gap. How do we make this decentralized payment system or that privacy that didn't quite make sense to me. So that's kind of how the idea of Iron Fish was born, was how do I focus on bringing more privacy into the space, such that the user does not have to give up private transactions or that their transaction history in order to interact with crypto assets?

Eric: Excellent.

And you also have you went on a podcast with zero, the Z KP podcast. I tend, sometimes I do a shout out for other podcasts. That was a, which was where I think I got introduced to, to Iron Fish.

Elena: Nice.

Eric: And I think I told you, I, I went to, to, to my son who, he's going into college, so I'm a, I'm a little older.

And I said, you got to like download Iron Fish and he's yeah. And then again, leading up to this, we actually got through everything. nice in the beta phase and moving forward on it. But I've been fascinated with Iron Fish since. And so this has been a, some time coming.

Before even kicking off into Iron Fish cause I think we touched on Z cash and there's other privacy projects out there. Look I know you have some perspective on, on the success that

they've achieved, how they've been used a little bit on their evolution. Maybe we could develop that a little bit before diving into Iron Fish and how it works.

Elena: Yeah. Great question. So when we started, the privacy space was pretty bare. So we had the older projects like Monero and Zcash, and then we had some newer ones, like grin was just starting out. Aztec was just starting out in 2018 era. And beyond that, there weren't very many now fast forward to today.

We have a ton more privacy solutions that are attacking the space from all sorts of directions. So there's some projects that are working primarily. And how do we increase privacy for Ethereum? So that would be, Tornado Cash, Aztec, Espresso if I'm not mistake or there might be some with some other is if I'm not, if I'm not.

For, from that for forgetting them. And so now we have actually Aleo as well is another layer one project. So we have this like suite of tools now that are attacking privacy from all different spaces. There are a lot of projects that are working on privacy on the Cosmos or the Polka dot ecosystem as well.

There are even some that are working on Solana. When we started, it was like very bare, barely any teams working on it. Now we're seeing teams experiment with, how do we have privacy with smart contracts? What does that even mean in the privacy space? Is it better to have a solution that is very focused on a particular chain, like doing a privacy solution for Ethereum Cosmos, Polkadot, et cetera. Or teams like ours

where can we build a more generic privacy layer that kind of integrates with all of them? So I think like it's really cool honestly, to see so many projects enter this space because we're seeing so many different attempts at what privacy means in a fairly transparent environment.

And the fact that we all have different approaches is really cool because we're experimenting what the public actually wants. And how do we make privacy seem less of a scary thing? Because if you talk to anyone outside of crypto, like their first kind of question is like this seems really scary.

Like how do you make sure that bad actors don't use your platform? And so the fact that we are having so much innovation in the space, I think is a really good thing.

Excellent.

Eric: So now we'll shift gears, and we'll start talking about Iron Fish and what you've experienced there.

How, what is Iron Fish? How are you looking to be different than some of the other projects, explain, how your offering is gonna be distinct.

Elena: Yeah. So we looked at the space and kinda like what I was mentioned before, there are a couple projects that are doing their own layer, one privacy solutions that are in my opinion, fairly siloed.

And I'm not, I don't wanna criticize any of these projects because we're standing in on shoulders of giants for sure. I appreciate everyone who's working in the space because quite honestly, privacy is extraordinarily hard to get. Not only from a technological perspective, but also from usability perspective, even a regulatory perspective.

But yeah, so we do have some, project like Monero and Z Cash who are, in my opinion, are like layer ones that are fairly siloed. Even Aleo I would say falls in that category as well. Then there is like projects that are in my opinion, too chain- specific. So there, there are certain projects that are offering privacy for only a particular chain.

And so for Iron Fish, the way we took the approach is we, as an industry, have the tool set for the best available privacy. How do we make it into this generic layer that any group, any crypto asset can actually use? So what we are doing at Iron Fish is right now, what your son play with, is a base layer

one chain that only supports private transactions. And the next kind of phase is how do we integrate with other chains using bridges, such that any curb to asset can be transferred from an existing chain over to Iron Fish so a user has the benefit of full privacy for any of their crypto assets?

Excellent.

Eric: And what's the relationship with Z Cash's sapling to Iron Fish?

Elena: Yeah. So we bootstrapped using Z cash is Sapling privacy mechanism. So to take a step back, like what is Sapling. So Sapling is a privacy mechanism that took an approach of a UTX so model, this is very similar to Bitcoin's model and use your knowledge proofs to encrypt transactions and have validations still happen in a fully encrypted way using zero knowledge proofs.

So what I mean by this is that using Sapling, you can actually make the entire transaction fully encrypted. So it hides the sender, the receiver and the amount, and the validation happens through an accompanying zero knowledge proof that says even though you cannot see the specific details of the transaction, the transaction is still valid.

So we took that privacy mechanism and built out Iron Fish around it. But Iron Fish is not a Z Cash for whatsoever. It's actually, from scratch and we can talk about the journey of how we got there. And so we really just took the privacy mechanism of Z cash and made that into kind of the core privacy mechanism.

Eric: Great. So we are gonna talk a bit about bridging, but I think, yeah, before we get into bridging, before we get into bridging, I think there's some evolution that we cover. And I think this is like a. , I'm not gonna say every part of the podcast for me is always fascinating. So it's not like I always have hard time.

This podcast is great. Every podcast I do is great. And I'm excited about all of this, but in talking to you in advance, we talked a bit about the evolution of the project, and I think, that's so rich just because you know how you progressed as an entrepreneur, thinking about different issues, pivoting on certain different points.

Obviously there's a lot of thing. There's a lot of thought that goes into those pivots. Cuz those pivots you can't take 'em lightly, you can't come in one day and say, I'm gonna do it different this way. And then come in the next day, no, you've got X number of pivots, if they're well executed project's better for it.

So let's take let's take a few. You started building in entirely in Rust and then you moved to Type Script. I always hear about Rust in these projects. I don't hear so much about type script. Of course, I'm not a developer, I'm a lawyer who has some technical capabilities, but like why did you make the change from Rust to TypeScript?

Elena: Yeah. Great question. So before I answer that, do you wanna say, if there's any entrepreneur listening to this podcast, feel free to reach out to me. If you wanna talk about your journey. Our journey in particular was very non-linear. We knew we were always gonna be focusing on privacy and we did, but the way we shaped the product has actually did did change over time, which is kinda what I'm about to talk the.

To talk to, but yeah, so we started entirely in Rust. Now Rust is an amazing programming language. If you've, if there's any kind of engineer that's listening out there is, it is a very strict language. It is now being used for a lot of security tools. So if you work at Square or even Dropbox or Facebook for some of their encryption stuff, like you will see some people using Rust.

And we started out with Rust also because some of the open source cryptography libraries that we wanted to use were also in Rust. Now the downside of Rust that we personally realized is that in our opinion, it was still a fairly developing language, and the open source ecosystem wasn't quite what we wanted it to be.

And our development speed was greatly impacted. Meaning that something that would anecdotally take us, three days to write in, like Python would write what would take us quite a bit longer to do in Rust. And so for us, we chose the speed of development. How do we experiment with our product much faster?

And we realized that Rust was not the answer. The other kind of portion for that was when we did raise our seed round and we were, ready to ramp up the team and hire more

people, we realized that hiring for Rust was very difficult. There are, they're not very many Rust engineers out there and they're very hard to get.

At the time the Rust community also had a weird relationship with crypto. Like when we talked to Rust engineers, they were actually very against crypto. So that kinda made it harder as well. And we realized that Rust is also a very difficult language to onboard. So if you're, if you wanna learn Python type script, Java script, even Java, you take some tutorials and you're off to the races. With Rust, there is a much, much heavier learning curve, which again, impacted our development speed.

So we made the somewhat painful transition from Rust to Type Script. Now we're not gonna get rid of Rust entirely ever. So 11% of our code base is still in Rust. But the majority of everything else is in Type Script. So when you think about what is a blockchain regardless of if it's a proof of work, proof of stake, proof of whatever there's really only five layers to any blockchain.

So one of the layers is networking. So how do peers talk to one another? The other is consensus. What are the rules that the network kind of abides to? One is transactions. Like, how do you make your transactions? The other one is accounts. And the fifth one is storage. So how does a node actually store the global state for your blockchain?

And so for TypeScript in particular, or actually for new blockchain, there's two bottlenecks, one of them is IO, so how quickly can you read from storage? And the other one is bandwidth. So how quickly can your network propagate messages? And so you can actually get fairly far with a non-optimal language, like type script and you can look at your bottlenecks and over optimize them in something like Rust, which is what we're doing right now.

So Rust is ironically creeping back into our enter code base, as we're looking to optimize some of the bottlenecks that we're seeing. So overall, I actually think it was a good decision because it made us move so much faster. It forced us to listen to our users. It forced us to over optimize on kind of a logical steps for how to make the entire system better.

And we were able to build so many more supporting development tools that let us, have more visibility into like how the note is operating. That I think would've been extra, like extremely hard for us to do in Rust.

Eric: And so if you had the whole code base in Rust, what would the advantages be? I'm sure there's others who would answer it, but like what tradeoffs did you have to make in order to do in order to go try type scripts, clearly there were advantages.

I'm just curious as to, what do you think some of the advantages of Rust, and I know you still have portions of it and maybe, yeah. That's what you're trying to optimize for, but what would be the advantage of having the whole code base and Rust?

Elena: So Rust is good for two things, correctness and speed. So correctness, meaning that, whereas other languages, especially dynamic languages, if you're listeners are familiar with what that means rust is a very strict language.

So the compiler itself will prevent the developer from making a mistake as, as much as possible. Which makes the developing portion a bit slower because you're fighting with the compiler . So correctness is definitely, a huge thing. So when you were developing code and Rust the language itself forces you to write your code such that it.

You're really minimizing how many mistakes the code could possibly do. That's part partly why, if you look at the heavy duty cryptography or security like libraries they're mostly going to be written in Rust. The other one is speed. So Rust is very good for threading.

So threading basically means, when you're running your program you have the ability to have separate tasks that be executed at the same time. And so Rust is a very greedy language. It takes all the resources from the host machine that it possibly can to make sure that your program runs as fast as possible versus in Type Script, you kinda have to use node, which is it runs your, like your program for you.

And so threading becomes a bit more difficult. And so you have to think. How you run your program a bit differently if you wanna have similar optimizations. So yeah the two biggest advantages there, like correctness and speed, for sure.

Eric: And it sounds like you're focused on where to optimize Rust for each of those along with the Type Script.

Elena: Exactly. Yeah. Type script is, like really great for other things. One of them is like readability and onboarding new users. Which I think is actually very important.

Eric: Hiring developers.

Elena: Yeah. No, but like JavaScript is actually the number one programming language in the world.

Like how cool is that? Like anyone, like if you were an engineer, anywhere in the world, chances are, JavaScript and type script is just an extension of that. So if we are trying to make Iron Fish be this open source library that anyone can contribute to then JavaScript or type script is actually the most logical language for us to choose that's what we're optimizing for.

Eric: Awesome. Great. Now at some point the team was building for the full Iron Fish node to work directly in the browser. That's where I got my son on. Yeah. But that's changed. Yeah. And why has it?

Elena: Yeah. So that was kinda like one of the pivots. So again, we knew we always wanted to focus on privacy, but how we wanted to focus on privacy has changed over time.

So one of our thesis was like, if we make privacy convenient to use and easy for people to use, then of course people are always going to choose privacy or non-private projects or we're not non-private solutions. And so we're thinking of, okay, how do we make a full node implementation, be so easy to run that anyone can run it.

And especially when we started writing Iron Fish in Type Script one of the things we chose for our networking stack is Web RTC. So you and I are probably using Web RTC right now to have this video recording call. So you know, every computer in the world kinda, Access to WebWork DC, regardless of, which router network you're using at home or not at home, et cetera.

And so the next kind of extension was why don't we make Iron Fish be so easy to run that it can run in the browser which sounded like a really crazy idea, because if you think about, running a full node, that usually implies you have a hefty machine to do and you're probably running a server and, probably requires a lot of storage.

And we did like rough math and realized it was possible. And we're really excited to do that. We also discovered a project called B coin which was a JavaScript implementation of Bitcoin. And we looked at some of the stats for B coin and in, I think, 2019 when the project was maintained it was the second fastest Bitcoin client for syncing speed.

And so we thought, wow, like this is amazing. This is a clear example; how not only can JavaScript run fast or be optimized. But you can actually have a full node in the browser. So we were really excited about this idea. And then we started talking to our users. We launched our Testnet and we, started asking users what they cared about.

And we realized that people didn't quite care about running a full node in the browser and they cared for other things. Like they were very much used to interacting with a command line. They did want a wallet kind of user interface, but they didn't particularly care if this, if it was full note of the browser or, something that was more familiar to them.

And so we realized that even though it sounded really cool, it wasn't extremely practical or useful for our users.

Eric: Excellent. And so now it's run from the command line and it's easy to use, but it's not browser based. So you don't run into all those issues. Then, I guess the third one to cover is also really intriguing is initially you hadn't looked at bridging to other chains.

I think it was all going to be self-contained like one, one L one, and that's it. Or my L one got. Yeah. And then you decided to expand a bridge to other chains. I think it's interesting, number one, why, but obviously we're everybody says we're in a multi chain world and , that I think maybe that's been covered, but also the, how you decided to go about the bridging cuz theirs, this podcast has had a lot has done a lot on interoperability.

And when I say a lot, we've had Raphael Belchior kind of walking through all the decision making processes for, how do you become interoperable? We had Thomas Harjono. We had Wan chain on talking about interoperability in bridging. But there's all kinds of bridges. And so how did you, number one, how did you decide that one's probably gonna be pretty quick and then how did you figure, how did you, what was your journey like to figure out how to go about, what solution what mechanism to use for bridging?

Elena: Yeah. So you're right. We did start as an L one. And at first our thesis was, if we make privacy really easy to use, people will come. And then 2020 happened and we saw an explosion of creativity happen in the DeFi space, NFTs happened. Daos happened. Lending protocols happened. There's just so much creativity that were, that was happening on Ethereum.

And it felt like we were intentionally building something that was so siloed and wasn't interacting with all this creativity that was happening in the space. So we quickly realized that people want privacy anecdotally, and also by action. And. We can PR we can provide really good privacy by bridging to chains like Ethereum and letting people have the ability to transfer their existing assets onto Iron Fish for full privacy.

It's really hard to convince that someone to sell their existing crypto assets that convince them to come into the space in order to buy Iron Fish, primarily because of the privacy, we realize that people wanna keep their current assets, but have them be in a private environment. And so the idea now is okay Iron Fish is actually extremely well positioned to be this core infrastructure layer for all crypto.

to provide privacy for all chains. And the solution that we came up with was to bridge to other chains and allow users to transfer their existing assets onto Iron Fish. So their existing assets can now have full bit full benefit of privacy. And then in terms of bridges, so bridges are a huge topic.

And I'm so glad that you had other kind of podcasters or podcast attendees take a stab at explain your bridges. I think bridges originally when they first came into the scene as a concept, even I think like in 2018, maybe they were a scary concept.

And a lot of initial bridges were fairly centralized, and people didn't really trust them very much. Fast forward to today, we have a ton of bridges. Every time you have a layer two,

there's actually a bridge that goes from a layer one to layer two, which I'm not sure if people realize layer ones to layer ones

we have a ton of bridges there as well. We have entire companies, billion dollar companies where, they're focusing on bridging chains to one another or bridging kind of transaction calls from one chain to another. We've also seen a ton of hacks. I'm not gonna go into all the hacks, but, and I don't remember the aggregates on money, but it's, it was, it is definitely an eyebrow raising some of money that was lost through bridges.

I don't think that's the end of bridges. I think like we, as an industry are learning some of the mistakes from those projects. And so for us in particular, we looked at this and said, okay there are, there's such a huge effort in the industry to figure out how to make bridges.

And we're learning quite a bit. And so for us, either we, as the company are going to maintain the bridges that I described or we would partner with existing bridge operators and convince them to provide, the benefit of people with bridging to Iron fish.

Eric: All right. So we're continuing this podcast a couple of weeks later, oddly, after the sanctioning of Tornado Cash smart contract addresses by the Department of Treasury and

coincidentally Craig Timm joined Iron Fish as their general counsel, and he is his story. So we're gonna continue with the background on Craig, why he moved into this space. And then we'll get a little bit into post Tornado Cash OFAC sanctioning. So Timm, welcome to the podcast. Sorry.

No that's okay.

Craig: Thanks for having me. This is great. So this is day two for me at Iron Fish. I spent the last six and a half years at Bank of America helping to lead their anti-money laundering program. So the program that banks are required to have to try to keep bad guys out in the first place. And when they get in, try to get them out. Before that, I was a prosecutor with the Department of Justice for many years.

Started as a prosecutor in Arizona, prosecuting drug cartels, and then moved to headquarters where I led what's called the Money Laundering and Bank Integrity Unit for the Department of Justice. And it is the unit that focuses on the intermediaries involved in money laundering. So banks, bankers, accountants, lawyers, and actually specialize in criminal violations of anti-money laundering laws and economic sanctions laws.

So not just where you violate the law, but where, what the law is, and you violated intentionally.

Eric: Great. And so now you've decided to join the Iron Fish team. Leap of faith into web three, or a different side of things. So what spurred that decision?

Craig: I think, it's a couple different things.

I think one, as I've learned more about the web three space in blockchain and cryptocurrency over the last several years, you can really see the potential or I started to better see the potential for this technology doing the same thing to finance as what it's done to travel, what it's done information, and that is make it faster, cheaper, better, and more accessible.

And frankly the big banks and the traditional financial institutions are just gonna have a hard time moving fast enough to keep up with the pace of change. And so I was interested in the space. And then as I learned more about what Elena and the Iron Fish team are doing, I really saw a chance where I could come in and help.

Cause I think, when you think about the traditional finance world or traditional government they're missing some pieces what's happening today. One, I think the lack of privacy that exists on blockchains today, don't think people appreciate that. Some of knows your wallet address, they see everything in your account, every transaction ever done, and, even more scary can follow you in near real time going forward indefinitely.

And so I think that sort of messaging along with, what does that lack of privacy actually do to facilitate crime? We talk a lot about, we talk a little bit later about Tornado Cash and privacy, maybe, helping the criminals, but it actually causes, the lack of privacy causes a lot of crime.

If you think about, the number one area of crime today in web three are scams of fraud. And the more publicly available information there is, you put out there about you, the better the criminals are able to target you. And so that's just you, one of the negative consequences from the lack privacy today. The second is just what are authoritarian regimes, frankly, gonna do with this unprecedented level of

financial data.

Eric: Great. Excellent. So exciting times, indeed. So now we're gonna get into the thick of it. The, what happened with the Tornado Cash sanctioning and even the arrests that followed it who wants to kick that one off?

Elena: How about I'll give a quick overview and Craig, please feel free to fill in the gaps.

So roughly a week ago we have got the news from the Us Treasury Department that they are sanctioning all of Tornado Cashes Ethereum addresses. And the consequence of that was that basically they were de platformed by, all major platforms that they were on. So for

instance, Discord de platform, them GitHub de platform them not only was the Tornado Cash GitHub account closed, but so was the founder's GitHub account closed.

And that alone raised the huge question of isn't code free speech? What is happening here? How is it that the US Treasury Department targeting a piece of code that cannot defend itself rather than an entity, an individual that was at fault for doing these crimes? And a few days later there was an announcement of an arrest of a developer of Tornado Cash in Amsterdam.

I do wanna preface that we don't have enough information to really jump to conclusions as to why this individual was arrested. And I'll let Craig give more color there, but all of this started this huge conversation in the crypto community of where do we draw the line?

And how do privacy preserving projects like Iron Fish and many others, how do we protect ourselves? We're all building this for the greater good. And so we all have good intentions in mind. And so this really aggressive reaction. From the US Treasury Department is definitely very concerning especially given that there's not clear guidance in terms of what precautions you should and shouldn't do.

It's more of, there's an invisible threshold that they obviously crossed. And so for us, we're thinking of, how do we react to this in terms of making Iron Fish way less convenient for, bad actors to use. So Craig, do you want to fill in some more gaps?

Craig: Yeah, I mean I think there is a lot we don't know. I think that there are two things that we can take away from the government's perspective. One, they viewed it as too much bad activity going through Tornado Cash. So estimates done that very interestingly in the press release the Treasury Department put out, they seem to imply that all of the activity going through Tornado Cash was money laundering. We know that's obviously not true. So not sure why that was.

The estimates I've seen, from some of the blockchain analytics companies is somewhere between 30 and 40% that known illicit accounts transacting through Tornado Cash. So I think we can take away that right or wrong. The US Government believes that's too much. And so that's one takeaway.

I think the other takeaway is around the controls that has mentioned where you, the press release also said, despite public assurances. The controls weren't good enough. So whatever we're doing in actuality, the US Government believed was not enough. So I think as we learn more about what those controls are, what those failures are, and this is arrest is a big question mark, right? Is this at all connected, right? I think there's a chance that it's not at all connected, it could be completely unrelated, or it might, might show some further intent. Like we just don't know. And I think until some of those additional pieces come out, it's really hard.

But I think the two takeaways for sure is, too much bad activity in the view of US Government, not enough control. So that's where, as an industry, we have to try to make sense of this while at the same time, certain groups will certainly be fighting. Maybe questionable legal ground for the sanctions.

Sanctions are typically against a person or an entity and their property. This code, as I understand it, I'm still new to the space, but I, nobody could change this code. The admin key was not functional, so it was no one's property. So how can sanctions apply? I think is the question that will have to be worked through, but I think there are a couple takeaways for now that we're thinking about and how we're building, how do we incorporate those.

Elena: In the statement,

so kind what Craig said, the biggest motivation for us USA for the Us Treasury to be so aggressive about it is because they viewed it as, North Korea, I think is getting something like 89 million, into the country per year annually because of sanctions and because of Tornado Cash they're able to get in, like launder close to a billion dollars.

Now, again, I'm not sure if that number's correct because I think that's a little bit over inflated, but regardless that's what they believe that through Tornado Cash, North Korea was able to launder close to a billion dollars. And so for them, it was actually a matter of national security. It was like, we don't know what's happening here, regardless of what they're trying to do in terms of compliance,

it's clearly not working because we're seeing the Lazarus hacking group, launder so much money through this protocol. And so they reacted very swiftly and aggressively. The other interesting thing about that statement was they classified Tornado Cash as a mixer and compared it to blender.io, I believe.

And what's interesting there is that it's technically not a mixer. Which is very interesting, like from a very technological perspective, it might have been used as a mixer, and I think that's probably how policy makers interpreted, because that's what they're familiar with. But if you look

at the tech of how Tornado Cash is actually built. It's actually way closer to Tornado Cash for instance, or sorry to Zcash than it is to an actual mixer. And we know that Zcash is not a mixer fundamentally by, by how it works. So it was interesting to see that regardless of how they were using the terminology, I don't think the terminology matters so much.

I think it's how it's used. I think what was happening in the background is that probably, I don't know this, but probably the Tornado Cash team was given some warning of look, we are seeing this bad activity happening on Tornado. What are you gonna do about it? And I believe their response to that was we are going to put some controls over our front end,

meaning again, I don't know, but presumably they probably geo blocked some sanction countries from accessing their front end.

But simultaneously they made a medium blog post that described how to use VPNs and why you would want to do so which was not a good look. They also had a compliance tool like on, on their website. So the compliance tool basically let you de anonymize a note. So the way Tornado Cash works is when you deposit something into the pool that amount gets transformed into a note or a record, I believe.

And so each record or note has a new key and using the website, you could produce a PDF that shows where the note came from and where it's going to. However, that is not on a wallet based level. It's only on the note based level. So think of it if you put in a $20 bill in there, you have a record of that $20 bill, but your account there's no like view keep per the account, so to speak which was again, kinda like halfway compliance and I don't wanna kick down a team that's, obviously going through it through a tough time, it's more like us analyzing what happened and how the US Treasury interpreted their efforts into the, like immediate actions that are produced.

Because clearly, if you are hacking group, controls on the website are not going to stop you. You probably are aware how to use VPN and what it is.

Eric: Yeah. That's for sure. Like the people who are most interested will figure out how to exploit it to their advantage, the best. Half measures, provide the back door, unfortunately, and then I think that's certainly probably part of the intent behind it.

So now we shift gears, but the dust hasn't settled, the dust is still hanging in the air, but, as a, as, as the founder, as a general council coming in, I'm sure, you are starting to think okay, what, what does this mean for the broader industry going forward?

What does it mean for privacy coins? Like Z cash, like Monero. What does it mean for a PFS where you can store, we can have smart contracts or cross reference and, not be centralized. What does it mean for what you're trying to do or others, how does it, impact the entire space we'll get to, we'll get to you specifically.

So we'll hit the bigger space and then we'll drill down to what you think it means for you.

Elena: It's funny that you said we're waiting for the dust to settle because what's happening. Is that when the function news came out, I think it was Monday of last week. So a week from now ish, a few days afterwards people started dusting famous wallets.

So you know, a lot of celebrities for instance, made ENS accounts which means like, their first name, last name .Eth, effectively. Or some other accounts that we know belong to celebrities. And so people have started sending a tiny bit of eth from the Tornado Cash pool to these accounts.

And by the sanctions order, technically these accounts are, now affect. And so what's happening is that protocols like Aave or DYDX are forced to block these accounts that have nothing to do, presumably nothing to do with this with any of this. They're technically now at tainted with Tornado Cash because people have been sending them.

It's I

Eric: think that's probably more of a tool issue than an actual risk of criminal prosecution issue. That's my understanding. It raises the issue, but it's a tuning, it's a question of how you've tuned your tools.

Elena: That's

the question of like, how far is if you are two hop removed from Tornado Cash, is that enough? If your three hops removed, is that enough? If it's clear that somebody dusted your wallet is that okay? Like how do you make that clear? So there are all these questions that are coming out of like, how do we deal with this?

And I was on a Twitter space that I think you participated in, and someone brought a really good point of yes, there might have been 30 to 40% illicit activity on tornado, but 60 to 70 was not illicit activity. Like people put their real money in there, like that could be their savings.

That could be like their, actual money. And so now you are blocking normal people from accessing their funds or from cashing out because the U D C like a circle basically, stop supporting Tornado Cash as well. And so those people are not able to withdraw their funds basically.

And so that raises, a really big question of how the crypto community reacts to this and what are the guidelines that we are putting in ourselves to make sure that regular people are still unaffected. And honestly, that's still a huge question. People are, clearly not aware of how to do that because you still can't use your account on Aave or D Y D X, if your account has been dusted, regardless of how obvious that's what happened.

In terms of IBF, I'm not sure how they're gonna react to this. And one concern that people had was, GitHub did de platform Tornado Cash. And so again, it isn’t code free speech? Why did that happen? And for could go kind of companies going forward. Do we use good hub as this main storage platform or something else?

So I have seen I think that's being mentioned in that regard. But I'm not sure how, they're gonna react to it. I don't think they much control over what actually gets put in IB pass. So I think from what I can tell, I think they are avoiding this argument or this conversation because it is messy to define what is right and wrong here.

But yeah, in terms of the greater crypto community, there is a lot of concern of how do you operate a business in this space? Because outside of privacy, preserving projects, kind, like I mentioned, like Aave and DYDX and many others. Now they have to adjust to this new reality as well of how like they have to put in some controls over their systems too.

And so they're trying to understand what those controls are and really where do you draw the line? Because before all this happened, the presumption was, if I launch a protocol and it's decentralized. And I don't have an admin key and it's actually fully decentralized and it's actually outta my control, then I don't have responsibility over it.

And that was actually the whole benefit of like host, of launching things in this decentralized manner. And now we are seeing that is not true. If you launch something, you actually are responsible over it as a developer, which is scary , especially how open source tools are being used.

Any tool can be used for good or evil. And a lot of people are comparing what is happening here to the crypto awards of the nineties, where the United States government said that encryption was a bad thing. It was, there was controls over the export of cryptography

And so Netscape actually had to launch an international version that had weaker cryptography that presumably NSA CIA could crack that and could seal encrypted traffic. So a lot of people are making comparison towards that of, how do we charge on forward, but make sure that we don't have a surveillance date and make sure that we still have a thriving crypto community without the burden of these unknown compliance expectations from teams that are just starting out.

Eric: So from the perspective of Iron Fish, as a builder, how what's changed for you over the last couple of weeks, I, you were already focused on this issue. So the changes that, that, that you're likely to have experienced in your thought processes are probably more nuanced, but what do you think, could you share

what those nuances are?

Elena: Yeah, so it's an interview podcast because our first session was before this news intersect session is after this news. And so I don't quite remember what I said, but hopefully it's consistent.

Eric: Yeah, I'm not gonna let you get out of it cuz I know exactly what you said.

Elena: Okay, great. So for Iron Fish, the tools that are already built in are view keys on an account level. So if an individual or an entity is receiving a subpoena or is receiving a request for an audit, they could use this view key to give, not just like one transaction, but the entirety of the wallet.

When we talked last time, I did mention that we want Iron Fish to be this universal privacy layer for all chains. And the way to get there is to have bridging from Iron Fish to other chains. And so in light of this news it kinda I'm personally jumping to solutions.

So this is like very raw early. We haven't thought too much through it, but like the US Treasury made it clear that look there's money from hacks that are being, that is being laundered through Tornado Cash. And so from the perspective Iron Fish, if we are going to be hosting that bridge or someone else that we partner with, we're gonna have either a holding period or something to make sure that there is plenty of notice for us, the team that is supporting the bridge to potentially censor the transactions that we think are in nefarious.

So whether that being like a 12 or 24 hour like holding period before the transaction actually get executed or something similar where, you know, it gives the team enough time to see, to see Is this coming from a chain address? Is this coming from an address that we know it, is irresponsible for hack and so

on?

Eric: Yeah I imagine that one thing I hear people talking a lot about is hops and velocity. the number of hops and the velocity of those hops. And I could envision a tool where based on the number of hops, there's like a whole period that is commensurate with, as you go, as you have less hops to a known bed address, the whole time gets longer.

Craig: It gets back to, I think,

basic principles of risk management, for both us and otherwise, you're gonna have to be able to demonstrate to the government and anybody else that you understand what your risks are, and every project will be unique and that you've assessed what controls are in place.

And as you, you hit a perfect example, right? One hop is risk less is riskier. Then five hops right? You're gonna have to demonstrate what those risks are and that you've got some controls in place to mitigate them. And that where you end up after those controls is in a reasonable spot. And the government clearly thought Tornado Cash crossed that line into unreasonable and took actions.

And so that's what, we're trying to learn as much as we can about, what the universe of those controls are and assess each one so that we don't get close to that spot.

Elena: Yeah. And I do wanna underline that. We are still gathering information. I don't think we have the full story yet.

We have witnessed the very aggressive reaction from US Treasury, and we have seen the report of the arrest, but we don't have all the information yet. And so it's really hard to jump to conclusions before we fully understand the why. We understand the why in terms of the Treasury or the government saw this as a national security threat, but we don't fully understand all the details that have led them to this conclusion.

And like this is still pretty, pretty early. And we're gonna see in the next coming weeks both the reaction from the crypto community of a pushback in terms of give us clear guidelines of what we can and can't do. And then we're probably going to be seeing more and more details come out as a fallout of from all this And we are going to get a more, more understanding of how the US government is thinking about crypto, especially in the terms of privacy.

It is actually going to force this topic of privacy, which, for us at Iron Fish, we've been waiting for a while. For people to really force the question of what we are allowed to have and what should we have and isn't privacy a right.

And if so, how do we do it in a safe, compliant way that kind of makes both the consumers happy. But also make sure that we aren't, that we're not crossing that line.

Eric: I'm gonna take a, I'm gonna go into the next question I had on this, which is gonna be maybe a tougher one, which is, what's the bullish case.

For the sanctioning of SC addresses. Now I'm not about to suggest that there aren't people who've, who's had their funds locked up and that there isn't, damage and pain being FA felt by yeah. Those in the crypto community. But, thinking forward in what it potentially means, there's a couple of different ways where, you could look at this, I know Elena on that Twitter spaces, I think we had it was Jim Greco was on there and he spoke about, he made a couple of points that really stuck with me.

And I'm not saying I'm a complete buyer, but one was, he thought it was very good for institutional adoption because continually Tornado Cash specifically would be brought up as a reason why, institutions wouldn't want to get involved in this space. Now, Tornado Cash isn't the only game in town.

So I don't know if we ever get away with, get away from that, nor should we try to get it completely away for that. Cuz then we're just traditional finance and we have all the intermediaries and costs, et cetera, all over again. And the second point he made that also stuck with me was, when we talk about 30 to 40% illicit activity, he said he made a point.

He says, could you imagine? And I guess Craig could probably respond to this even better. Cuz he specifically used like JP Morgan or Bank of America as a, as an example. And he said, could you imagine if it came out that bank of America had 30, 40% illicit activity, can you like, it would be complete chaos and he says, it's very hard to say there's 60%.

That was illicit when there was, or 60 to 70% when there was 30 to 40% that was illicit. And it was it was a compelling point. He certainly, a lot of kudos to him because obviously it was it was a circle that wouldn't be receiving that message from him very well. And then I think maybe another argument, although I have to think about it again.

I'm not trying to say it was a good thing. I'm just trying to say what's a Contra case is arguably by doing this, OFAC has set the precedent for recognizing smart contracts, as people, as persons under the law, which is a very intriguing concept. And I'm not saying that we're gonna go from this to smart contracts becoming entities, like the Wyoming smart contract LLC.

Right. I don't think we're gonna move to that world. I'm I love Wyoming, so I'm not picking out any say, like they're like one of the more avant garde in, in terms of regulation. So I thought that was intriguing. I don't, again, it's an interesting precedent. It may impact future discussions.

Hey, you treated them as a person here, why wouldn't you treat him as a person there? So anyway, those were two thoughts that come to mind, but interested to hear what do you see as a potential again, I'm not saying it's all bullish, what would you say are the potential positives that come out of this?

Elena: If I can take a stab and then I would love to, oh, love for Craig to join in as well. So my bullish case for this is I'm partly glad that the reaction towards Tornado Cash was so aggressive because it really made the crypto community wake up and start having these conversations and debates out in the open.

And the Twitter spaces actually outlined this perfectly. If you remember the, the docket list of all the speakers they were not just influencers, but, we had a from TRM labs, we had VCs of other privacy preserving crypto projects in. We had people who were from GCs from other crypto projects as well.

We had people who were influencers. It was a really strong list. And it did make the crypto community kind of band together and figure out what is happening here. What, and how do we move forward? So my bullish case is that it will force a lot of clarity on how crypto project should run.

And again, this is not just privacy preserving crypto projects, because it does raise a concern for, basically any other defi project that deals with users of how do we have certain controls and what does the us government deem as a bad actor? How do we get that information in time? Your questions from before of if we know a bad actor is here, the wallet is three hops away.

What do we do there? So I think it'll start forcing people to have that clarity, which I think is really good. The other kind of comment he mentioned was the institutions are going to be

scared off or that they were scared off because her cash was in the area. I think the opposite is true.

I think most institutions want privacy because that's how they operate in the real world. Again, I don't think people understand just how transparent crypto is your, your entire quote, unquote being statement is out in the open with crypto. And I think when people realize that they're like, oh, wait a minute, privacy is not a dirty word.

It's actually getting me closer to the same financial privacy expectations I have today. And then for your other question, I'm gonna let Craig answer that one.

Craig: So I completely agree with Elena on, the benefit of bringing this privacy discussion to the forefront. I think that the dusting actually helps some of that.

Cause it illustrates some of the challenges and how legitimate people get caught up in this and right. How do we protect that? I also think an alternative bullish view would be, look, the Lazarus group is targeting our community, right? Like they're stealing these funds from web three projects.

And so the government as is saying at the same time, that's not acceptable. And we are going to use the tools that we have to go after these hackers that are targeting us where, our users are victims, they're losing funds. So it, it, it doesn't mean that their sanctions are in this case are right

or even legal maybe in some cases. But I think, it, while we feel there's a war on crypto and there may well be, they're trying to fight a cyber war at the same time. And we're one of the victims of that war, too. So I think it's just a lot more nuanced, I think, all around than black and white here.

Eric: And obviously I think, I don't think there's many who believe that OFAC is suddenly gonna say, okay, we screwed up, we shouldn't have thrown Tornado Cash as smart contracts, sorry guys. Forget about it. We'll move from here. I don't think anybody believes that's gonna happen.

There may be challenges. There may be specific challenges and, I think those challenges are healthy because the next question is if they sanctioned these smart contracts on Tornado Cash, what's next, and how aggressive do they feel about using this tool? And if that's the case, then it really sends this

it really has an incredible chilling effect because, while now we're trying to figure out and the dust will settle and we'll figure out how to, hopefully there'll be ways for people who've been hurt by this who are illicit not illicit, but licit exchanges will be able to get their funds unfrozen, et cetera.

The big question is the potential chilling effect going forward. If this is a tool that suddenly OFAC feels like, oh, you know what? We done this smart contract we should sanction, or that smart contract, we should sanction. Without clarity it, it does have a chilling effect.

Elena: Yeah I Don't remember the exact analogy that someone brought up in the Twitter spaces, but this is analogous to, like if Steve jobs were alive, like if someone did a crime on the iPhone, then Steve Jobs goes to jail.

in a way, that's what's happening, and again, we don't have all the details. We don't exactly know why the developer was arrested who was connected with Tornado Cash. But that's the analogy that people are using of, if I am putting out open source code and that open source code gets used for nefarious reasons

it is very scary if the author of the open source code was deemed responsible when they had, technically no relation to the actual crime that has occurred.

Eric: And it really gets into the whole question of what, that is a very ne- while there could be elements that are bullish, certainly what it does,

I think it's obviously outweighed by a lot of the other considerations, which is what does it mean for the developer community? What does it mean for who's next? The willingness to use that as a tool and just, even what it means for, freezing of other people's funds now in, in sort of anticipation of this and not knowing how many hops. So any other thoughts before we break on this this Tornado Cash shaking of the snow globe.

Elena: I guess my final thought is crypto can't go forward without privacy. So whether it be us or Aztec or Espresso or any of the other teams that are working on privacy, privacy is a must for crypto to be its fulfill his, his final dream. We're, as a community are going to be figuring out these questions.

It that's pretty inevitable, there, the future's probably going to be some middle ground of privacy with compliance. And that's all, very much what we're working here on, on Iron Fish.

Craig: And it, this it's not going away. And so I think the US Government, as they, they think through this and think through their next response is, the technology is there, it's out there. It's gonna be deployed somewhere. If you're the US Government, I think you want that innovation here. I think just like they ultimately concluded with the internet and the encryption wars the first time around, better to have it here, better for the American people, better for the American economy.

And we're an American company that wants to be here, we wanna work together and we wanna figure out the right way to do it.

Eric: Yeah. And we also have to, on that point, there's also the SEC involved in that one as well, but yeah. Listen, it was great to have you both back, the timing of our podcast.

I feel like it was like the perfect setup for this. I feel like we were just, we were all set up and then it happened, then it's okay, we're just gonna pick up and now continue with what happened with the sanctioning. So again, thanks so much for being on The encrypted economy. Appreciate it.

Elena: Thank you so much.

Craig: Great!