diffuse*tap*
Virtual Event Series

Keep Your Crypto Safe

Guest Speaker:

Frances Zelazny
CEO & Co-Founder
Anonybit

Hosts:

Kenny Estes
CEO & Founder
Diffuse

Ayla Kremb
COO & Co-Founder
Diffuse

DiffuseTap: Keep Your Crypto Safe

Last time on DiffuseTap, **Frances Zelazny, CEO and Co-Founder of Anonybit,** talked to us about how different cybersecurity measures are being implemented in the world of Web3, the difficulty in finding balance between anonymity and security, and why Web3 might not be as decentralized as you've been led to believe.

Want to make friends from the Diffuse Fund Ecosystem? Email contact@diffusefunds.com.

DiffuseTap

This networking session is part of our weekly virtual events series. Networking (you'll bump into at least a dozen high caliber fund managers) meets purposeful (you'll tap into brand-new sources of ideas)... straight from your armchair like a boss.

Meet the Speaker

FRANCES ZELAZNY is the Co-Founder and CEO of Anonybit, a new venture that focuses on developing decentralized biometrics technology to protect consumer privacy and enhance digital security. Anonymity provides a solution that makes personal data unhackable and ensures strong authentication without maintaining central honeypots.

LinkedIn: @franceszelazny

About Diffuse®

We are an alternative fund platform offering differentiated investment products. From digital assets to VC funds and beyond, we identify green field investment opportunities we feel will have market beating returns and turn them into professionally managed funds. For more information, visit www.diffusefunds.com.

KENNY ESTES: Ms. Frances, would you mind telling us a little bit about you and what you're up to over at Anonybit?

FRANCES ZELAZNY: Sure, thank you so much for having me. This is such a fun group. I'm Frances Zelazny, and I have been in the biometrics and identity space for more than 20 years. I helped grow one of the first facial recognition startups into what is now a global enterprise. We're involved with every single aspect of identity management and biometrics. Suffice it to say, I'm happy to answer any questions around those general technologies.

I've been involved in promoting responsible use guidelines for biometrics and, by extension, privacy regulations around biometrics. I'm very passionate about identity for Web3. As I just mentioned in my great breakout group, I see a lot of mistakes being made in the world of Web3 that I think, with like-minded people like yourselves, it's still early enough to try to address those so that we don't create a big mess down the line.

Anonybit is the brainchild of myself and two partners. We formed the company squarely around data protection, and protecting personal data and digital assets. We built a decentralized infrastructure that manages biometrics images and all kinds of personal data. And on top of this infrastructure, we built two products. The first one is a passwordless authentication solution built around decentralized biometrics, and the second one is a decentralized data vault, which manages any kind of other personal data.

These two products work hand in hand, which I'm sure we'll get into in the discussion. The idea is that today, fraud happens because we store personal data in a central honeypot that hackers can get into in order to impersonate us when they want to get into our accounts. The same holds true for Web2 and Web3. It's just that in the world of Web3, there's this whole notion around privacy and anonymity, and that everything should be decentralized.

These concepts start to come into conflict when it comes to security, and I'm sure we'll get into that. So again, thank you so much for having me. I really look forward to the discussion and to being in touch with you all in the future.

AYLA KREMB: Awesome. Thank you so much for the really neat and thorough introduction to what you guys are up to. I'll jump right into the questions here. What is crypto security? What does it really mean? Is that identity? Is that DeFi audits? Is that AML and KYC? What is crypto security in your world?

FRANCES: I think we could just take a step back and say, what are the pillars of cybersecurity in general? And then, how do they get applied to crypto? Within the world of cybersecurity, there are generally five pillars, if you will, and they're all somewhat interconnected. I'll give the textbook answer first, and then my interpretation. The five pillars are confidentiality, integrity, availability, authenticity, and

non-repudiation. Generally, when you talk about cybersecurity, those are the five elements. But they all boil down to two several concepts. And like I said, they are all interrelated.

Confidentiality is really about data protection. Where is the data stored? How is it stored? How is it encrypted? How is it managed? Who has access to it? and so on. It's important. The second one is integrity, where you're managing data to make sure that it is kept in its original form, and the form that it was intended. That was actually where blockchain originally started, with this whole idea that you can have data being recorded, and you know that it can't be changed, and so on and so forth.

I spent some time in the world of behavioral biometrics and fraud, and I learned a lot about malware and how you can have malware injections that change the intent of a certain traffic of information. It's really quite scary, because you might think that you are making a transfer to one person, let's say $100, but there could be a malware script that will redirect the trade into another account in real time. So, integrity of information, and integrity of information transfer is the second important aspect.

Availability is all around ensuring service uptime, which includes the denials of service, website crashes, and all of that. That's the third pillar. The fourth one is authenticity. Authenticity and non-repudiation are the two that are actually very close to my heart. Authentication revolves around who is authorized to access the information, and how do you make sure that the authentication process is handled properly.

Passwords are not a good form of authentication because they can be lost and stolen. A lot of mechanisms today are not really good, strong forms of authentication. When people think of authentication, they think of three things: something you know, something you have, and something you are. Something you know can be fished out of you and can be stolen. Something you have can be taken over by a hacker. Think about sim card swaps and things like that. The only one of the three that cannot be stolen or taken over is your biometric, which is something you are.

And so, when it comes to strong authentication, even though we talked about needing two factors for best practices, one of those factors should always be a biometric. We'll get into that on the non-repudiation side. You want to make sure that you have proper authentication both on the sender and the receiver side.

Back to that malware example. You want to make sure that the person who is receiving the money is really the person that you are intending. This also comes up a lot in the world of crypto because again, the whole notion of anonymity, privacy, and things like that is you're not really confident about who the person is on the other end that is conducting the trade. These are the five pillars of cybersecurity that play directly into crypto security.

KENNY: That's great. We'll keep it high level for the next question. Why does this matter? It's crypto, right? It has to be pretty secure. That's the whole premise. But is that actually true? What are we seeing? What are some of the horror stories that you've seen as far as where these things go terribly awry? What's the pain point you're trying to address?

FRANCES: Yeah. In the world of crypto, there are a couple of pain points. I would say one of them starts with who is opening a crypto account. Most of the regulations and most of the attention has been there on the KYC and AML aspect, but there are problems with this. These are things that happened in the world of Web2, and that are happening in the web world of Web3 for sure. You have people that are acting as money mules.

They are opening accounts, and they're using these accounts to move money around on behalf of illegitimate people. That's one thing to look out for. And because all of these processes are happening separately, you actually can have multiple people operating under multiple identities. You actually may not know who you're transacting with. It might seem like a legitimate interaction, but what's happening in the background is not necessarily well known. From a regulatory point of view, in terms of making Web3 and crypto a safe place, this is an issue for synthetic identity and for identity theft.

The second issue is the assets themselves. This is something that I think is a big problem where you have assets, whether it's crypto assets or digital assets, that are not necessarily bound to my identity. Anybody that can take control of my wallet will have control over my digital asset. This, to me, is the second danger.

The third one is the wallets themselves. I don't want to embarrass anyone, but I imagine that a lot of people on this call write down their private keys on a piece of paper, or store their private keys on a fob. And then, if it gets lost, we all know what happens. None of us want to be the one that had to sue the government. I think it was in Quebec where someone had to get into a landfill because they threw their FOB away. The whole notion of lost and unrecoverable wallets is actually a big problem for the good guys.

I think there's a lot of issues. These are things like where the rubber meets the road. How do you make sure that you have proper wallet protection? And how do you make sure that when you need to access it, you actually can? These are the three issues of why this matters and where things get into hot water in my opinion. Kenny, do you want me to answer the question in the chat?

KENNY: Sure. I'm not going to paraphrase this next question for you from the chat, just for the people who are listening after the fact. Basically, there are different types of biometrics. You have facial recognition, voice recognition, fingerprints, and eyeballs (the latter two in spy movies tend to end pretty graphically). So, what are the various pros and cons of the various biometric solutions?

FRANCES: They're different modalities, and there is no single modality that is perfect all the time, for a variety of reasons. I'll just make it very obvious for the person who asked, Henry. I think we know each other from before. Henry was asking about voice biometrics when you make inquiries in banking. This is obviously a call center application, and if it's noisy, it may not work as well.

A voice also does not work well for what we call a one-to-many solution. You can't do a "let me see if I know this voice from before" and run a query. But it's very convenient. One of the main benefits of voice is that you don't really need to train the voice. Just like how we're talking right now, a voice recognition

system can just pick up inflections and whatnot and make what's called a voiceprint and use that as a mode of biometric recognition.

What we see is that today, everybody has cameras on their phones. So because of phones, face tends to be the primary and voice tends to be the secondary. With face recognition, you can use it on your own and you don't really necessarily need to do anything. You don't need to call. It's more of a self-service. And also, you can leverage the face ID, which is a lot. I don't want to get too much into the technicalities here, but I would say that face ID is much more ubiquitous. But voice is also an excellent secondary biometric.

I want to address the question in the chat around biometrics being stolen or hacked, because this is actually a really sensitive question and something that is really hard on a personal level. It's the impetus for the creation of Anonybit. The answer is yes, there are certainly examples of biometrics being stolen and hacked. The U.S. government office of personnel management database had fingerprints that were hacked, so this is a very sensitive issue.

I know this is not meant to be a commercial for Anonybit, but I'm just addressing this question. One of the reasons we formed Anonybit was to fix this problem and to decentralize the storage of biometrics information such that they could not be lost or stolen. We don't do this on the blockchain because when it comes to biometrics, you actually need to process data. Instead, we leverage multi-party computing and zero-knowledge proofs in order to do this.

That way, we can store biometrics such as face, finger, iris, or voice within the multi-party computing network such that it never actually comes back together again. It cannot be reassembled. Even if one component somehow gets accessed, it is not related to any other component. It's our mission to address this relatively new aspect. This is where our patent is.

The big question is really about consent. When it comes to biometrics, biometric data protection laws don't generally touch on several aspects. Number one is that consent collection has to be done with consent. Well, BIPA is all about consent, and says you should not collect biometrics without user consent. Every single lawsuit with a BIPA judgment has to do with this.

I drafted privacy regulations back in the day and there should be user consent especially for when it comes to commercial aspects of biometric collection. In addition, we need to consider spoofing and deep fakes. There are technologies that are designed specifically for that. Liveness detection and deepfake detection are areas that are very active in research and development, and are some of the things that are built into our products. We use third parties that are specifically working on this. I'm very happy to share any further information on that.

With regards to crypto anonymity with biometrics, it's the idea of keeping your identity. It's not about anonymity. As I started to see before, there has been this mishmash of privacy, anonymity, and security. We need to make sure that we understand these definitions because this is what gets us into hot water. Privacy is keeping something to yourself. Privacy is, I have my identity information. You might have my identity information, but this is not necessarily meant to be shared or publicized.

We need to keep that secure back to the pillar of cybersecurity and data protection. The information about my identity can be kept private. That's different from anonymity, which means I'm doing a trade,

but you don't know who I am. I think this is where things get dangerous in the world of web3 and where the illegitimate stuff happens. You don't know who I am, and I'm doing all of these things. I could be a money mule. I could be a terrorist. The bad guys thrive on anonymity.

But you can still be secure and have your identity established and registered, but have it private and not completely anonymous. How you do that is with KYC and AML. That's happening, by the way, just so everybody's aware. KYC and AML is being done in crypto today. But so everyone is aware, on the back end, all of the data that is collected is stored in a centralized database.

People might be issuing verifiable credentials and saying, “Okay, you have an identity token.” But on the back end, there are these giant databases. Again, this idea that we're anonymous or private is actually not true. These are misconceptions. So, how do you do this? You can do this by decentralizing those backend databases. That information should not be in any centralized honeypot. You can issue verifiable credentials for people to transact. That's how you maintain privacy.

When you do a trade, the transaction should be verified biometrically, not with a password that somebody else can steal and take over. Or your mother's favorite color, or the street you grew up on, or other information that is very widely available. Because when people say, “Okay, how does your wallet get taken over,” this is exactly how it happens. We need to separate the three concepts and understand how to create security amongst those concepts.

Thank you for downloading this DiffuseTap event transcript.

Sign up for upcoming sessions and check out past features and event transcripts.

Dennis Chookaszian

Corporate Director, CME Group

DiffuseTap: Institutional Grade Governance

Sharing his decades-long expertise on corporate governance, Dennis talked about how to avoid a co-partnership going sour, the problem with overly idealistic CEOs, and the importance of keeping your board in check. Read on

Susan Brazer

CEO & Founder, LionShare Media

DiffuseTap: Media Metaverse 2022

Susan described the 2020 digital media landscape; the evolution of media distribution; how converging, emerging technology points to the metaverse; and the prospect of having an open, decentralized, and free Web 3.0 marketplace. Read on

Raj Mukherjee J.D.

VP/Global Head of Tax, Binance.US

DiffuseTap: Crypto Taxes Decoded with Binance.US

Raj explained the complexities of the US crypto tax landscape, how he built a dynamic tax information system for Coinbase and Binance from scratch, and how investors can profit from crypto without getting caught in a taxation mess. Read on

JOIN US