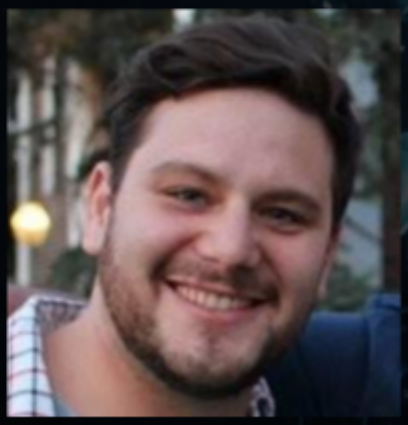
diffuse*tap*
Virtual Event Series

Gaping Crypto Security Holes

Guest Speaker:



Eric Freeman
Co-Founder
Magellan Security

Hosts:

Kenny Estes
CEO & Founder
Diffuse

Ayla Kremb
COO & Co-Founder
Diffuse

DiffuseTap: Gaping Crypto Security Holes

Last time on DiffuseTap, Eric Freeman, Co-Founder of Magellan Security, talked to us about the weakest link in all crypto projects and exchanges, why blockchain technology's reliance on web2 infrastructure is holding it back and leading to security risks, and the reason why great crypto insurance policies just don't exist yet.

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

ERIC FREEMAN is a Co-Founder of Magellan Security, an advisory and consulting company that protects and strengthens security for small and medium sized businesses. With experience in SaaS, fintech, blockchain, and traditional enterprise companies, Eric has helped implement and scale security programs tailored to the business model of their clients.

LinkedIn: @eric-freeman

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: Mr. Freeman, please tell us a little bit about your background and what you're up to over at Magellan Security.

ERIC FREEMAN: Awesome. Pleasure to meet everybody here. Hope everyone is enjoying spring as it springs itself out. My name is Eric Freeman. I'm based in a small place called New York City, and I've been working in security for probably around a decade or more in crypto, blockchain, web3, distributed ledger technology, or whatever you want to call it for about six to eight years now.

I got into the space because early on in my career, I was what is referred to as an incident responder, where my company would be called after there was a breach. Not Magellan, but the consultancy I was working in at the time. It was very early on during the ICO boom, and many companies that were raising funds were getting their marketing pages hacked with default credentials and having their wallet addresses changed. And so, we would come in to help do forensic analysis.

At that time, I saw that this space was not only both quickly growing, but it also did not have a lot of controls, a lot of processes, or many ideas of how to think about security. It was very early on in smart contract days. We didn't have layer two or layer three as we do today. What I've seen throughout my career is one, a lot of companies focus on what they think is web3 security, which really comes down to custody, private keys, private key infrastructure hardening, as well as just maintaining your assets the right way. But there's a lot more to it than that.

I think if you did a deep dive into it, based on what I've seen at BlockFi where I worked previously and Blockdaemon, most of these companies don't think about the basics and web2 security. The reality is that the weakest point of any company is our staff. It's insider threat, and it's the risk that can be posed through your own team members and your own staff by not having the right process controls and risk models in place.

And so, I'm here today not only just to help guide some conversations around security in the way you guys should be thinking about, but ideally help people that will serve as a resource and an expert in what we should be doing to not only better educate our customers, but also our teams around us.

At Magellan, we really focus on helping scale and harden fintech companies, startups, and web3 companies. We work with various funds, apps, and decentralized apps, and make sure they're doing the right things as we enter this space that's rapidly changing day by day.

AYLA KREMB: Beautiful. Maybe we can dig into the weakest link. What is the weakest link in crypto security? I'm sure humans are one, but maybe the infrastructure is another?

ERIC: Yeah, it's a great question. The weakest link is always the staff. And then, it's how the staff accesses their information. When we're looking at a lot of these companies we're working at, it's a remote world. And it's not just in the perspective of your company based in the US that has staff all over the place, but with a lot of these blockchains and the code that's being written, we're talking about people who are

contributing to open source in this gig economy all over the world. Most of these projects are from people based in Southeast Asia, Eastern Europe, North Africa, and South America. It's really decentralized. And so, ensuring that the person is indeed who they say they are is critical.

One of the biggest things that we've seen through my network of the intelligence community, as well as what I see on a day-to-day, is that a lot of networks blockchains ecosystems are getting targeted by having someone that they think they're bringing on as a developer, but indeed, is really a nation-state threat actor from either North Korea or China. They are building malicious code within these projects to be able to have something that they can execute from a vulnerabilities perspective.

So, to answer Ayla's question directly, it really is insider threat and insider risk, which is how do you know the person is who they say they are, especially in this pseudo anonymous world that we're in that really prioritizes itself on privacy? And also, how do you ensure that the code that you're integrating with the blockchain and the apps are what they say they are? Which comes down to the infrastructure side, which is how are you scaling your infrastructure and integrating with these blockchains in a secure manner.

KENNY: That's great. It's funny because you see all these stories about people who are getting 10 developer jobs doing no work, and then they just take a salary for six weeks and then get fired. That just shows how easy it is to get a job, I imagine, as malicious nation state actors are not having a hard time getting in the door. That's absolutely fascinating.

Another area is around more traditional web2 type security, cloud security, and the wallet management or distributed organization, and what people need to think about there. What are your general thoughts on the vulnerabilities there?

ERIC: That's an excellent question. I think the one thing I want to call out here is with the fall of FTX and the administration pushing in a very specific direction, what we're going to start to see not just in the US, but also in the Middle East, Southeast Asia, and Europe, are two real frameworks. I'll bring this up because it's important to explain how this pertains to cloud security.

One, you're going to have heavily regulated entities that want to follow the rules and operate specifically to what the regulation is going to be. That is going to involve things like custody, having MTL licenses, and ensuring you're doing KYC AML. It's making sure that you're doing the right things you would see of a traditional bank.

And two, there are going to be unregulated exchanges like DEXs. These are completely decentralized and segmented. When it comes to cloud infrastructure, the way that these two types of entities manage it is completely separate. Most exchanges and DEXs operate with a foundation at the top level, where they manage the infrastructure and manage the tools. I can give you two examples. One is OP Labs, which maintains Optimism, a layer two on Ethereum. Another is Filecoin, which is part of Protocol Labs. They

maintain the Filecoin ecosystem. These are entities that are based in the US and have staff, but manage the infrastructure for the blockchain. That's decentralized.

When it comes to centralized exchanges, it's a company that manages the resources. When it comes to cloud infrastructure, you're still relying on AWS, GCP, Azure, or other bare metal providers to stand up these nodes and to build this application that you integrate and interact with for doing trades.

When it comes to cloud infrastructure, the most important thing you have to first think about is one, who's accessing your cloud infrastructure. You may be administering permissions to a developer, an SRE, or a technical resource. But the reality is, that's still the foundation of the network. Just because it's decentralized doesn't mean that a large entity isn't still maintaining the backbone of it.

Yes, they rely on people to stand up nodes. They rely on other infrastructure companies to help build nodes to support that blockchain or that company. But the reality is it's still somewhat centralized. Through that, when it comes to cloud security, the next component is the trading engine and the wallet management. I've heard somebody mention today that they use Fireblocks.

I'm going to mention because I've worked at a company that had Fireblocks as a back engine. Fireblocks does not create backups of their customer images. That's on you. So, something to think about is where you are storing your backups. Are they on the cloud? How are you managing it? Most of these wallets are built with cloud service providers. Whether it's using something that's referred to as computational secure compute resources that are hyper locked down, you're still using code and automation to gather these private keys.

So when it comes to security, it comes down to what is the best way to create an M of N, or a certain amount of shards that you delegate and that need to come together to be able to create the private key at your company so that you never have risk to your wallets. And most of the time, these people are deploying their wallet infrastructure on the cloud.

I brought up the regulatory issue upfront because we're going to start to see over time that this is going to change in how it's managed. That's because you are going to have to meet requirements of what the government is going to say when it comes to custody. And that's super important because it directly impacts customer funds, which is going to be a key component of how you scale either your decentralized exchange, your centralized exchange, your trading engine, or your trading algorithm. The cloud is where all this is deployed.

I think that people get lost in this concept of decentralization. But no matter what, you're still relying on web2 technology to build your platform, scale your platform, and get your application and code out there.

AYLA: Superb. That was quite the essay. Maybe we'll dig a little bit into that because we have some questions around hardware wallets and securing them. Is that enough or not? Maybe you can touch a

little bit on that and dig into the details, because I think some of the folks here might be believers that the hardware wallet is a really safe place to put your assets.

ERIC: It's super interesting. I'm a huge proponent of hardware wallets. I have five different ones in my house that I use on a daily basis. I think the more factors of authentication, the better. But I also think it depends on the use case. I say that because a hardware wallet for an exchange is not going to work. They have to have warm funds that are ready to be withdrawn for their customers at any point in time.

That's where something like Fireblocks, Anchorage, or something a little more institutionalized that has a warm solution is going to help scale it as it pertains to your private funds. It's super important to not only have your wallet, but make sure you're using browser plugins to help check what you're engaging with. I say this because when it comes to using and integrating with DEXs or any type of bridge, you need to make sure that that bridge is indeed what it says. There are great applications like Wallet Guard, Revoke Cash, and other third party plugins that are used to check the calls that are being made.

That means the wallet is great, but you're still granting access to that wallet when you're making trades on decentralized exchanges, and granting authentication capabilities and privileges to the application. And so, what I've seen in certain circumstances is people may have a hardware wallet that looks live and ready to go. But the reality is that they have an app within Metamask that it is integrated with. And what happens is, that application is indeed vulnerable or gets breached, and the attacker is able to access the funds because the wallet is live.

But that's just one component. It's not the entire story. I think it's super important to have a hardware wallet. Again, I have a bunch of them. And it's also important to segment your funds in a way to limit the amount of risk you're willing to take on based on what your portfolio looks like. I divide an even amount amongst all of my wallets.

I also use a great wallet that I love called Oculus. It's a 3FA wallet that isn't necessarily as easy to integrate with Metamask or Trust Wallet. But what it does do is it gives you a mandatory way of having three steps of authentication to be able to access your funds. In short, while it's super important, I think the hardware wallet is critical, and implementing the max amount of MFA and friction.

But when it comes to standing this up for an organization, it's not necessarily what I would recommend. It's great for a retail user or an individual, but it's not great for companies. I think there's a better conversation to have around cold storage when we're talking about those use cases. If you're going to backup funds in another place for a company, that is good. But sharding the keys, which means taking what the seed phrase is, encrypting it, breaking that up, dividing it amongst a company where people don't know what they're doing to avoid collusion and they don't know who has it to bring them together, is one thing to think about and consider when it comes to backup funds.

KENNY: That's really interesting. We'll go further. Obviously, one of the big risks of hardware is if you lose it. So, where do you see the industry going? I'll pick up a question in the chat here. Do you

see a future state where there is a custodial layer, where there is a layer that sits on top of all of the individuals who are managing the private keys, and they manage it in a way that people are actually safe and secure and institutionalized? Or is that just more of a pipe dream?

ERIC: I'm going to bounce this question again back to the bit about which way we are moving towards. It depends if you're a regulated entity or non-regulated entity. I say that because non-regulated entities are big on self custody. It's almost the ethos and the driving force behind this ecosystem. I'm talking with one potential customer right now that's trying to build the Amex of crypto, as they claim. But on the back end, they're trying to build this on this concept of self custody. So, as it pertains to B2C, it's largely going to be self custody.

I think it comes to dealing with larger institutions like BNY Mellon or Bank of America, because they're larger banks, they are going to be much more reliant on not having self custody because that's how they built a lot of their foundation of the economy and their banking operations. And so, I think it's going to come down to one of two things. Do you want to be operating in a regulated way? I think there is a lot of risk that is associated with the consumer in the West. And with those regulated entities, I think it's going to be largely traditional custody as we know it.

But when it comes to unregulated and more B2C non-traditional users, it's going to be largely self-custody. That's what we've seen, and that's how things are being implemented. I've had to audit a lot of these custodial providers like Fireblocks, BitGo, and Xapo, and other companies that have come and gone, and also the ones that are working with these large institutions. The reason why is because they are qualified custodians that need to be able to maintain their assets on behalf of customers. It really comes down to the regulatory component of this, if you ask me.

AYLA: Fascinating. There is a lot of scope there. You said "Amex of crypto". Could you dig into that analogy a little bit?

ERIC: Yeah, well, that's specific to a product that they're coming out with. That's what they claimed to me is what they're building. It's a really easy, accessible, somewhat rewards-based self custody wallet that allows you to get points every time you do a transaction. They do a percentage of what comes back and a reward of some type of token. I don't have all the details of that. But it was more specific to this company that I'm talking to and their philosophy around self custody.

KENNY: Gotcha. Another question here from the chat. Are you working with insurance providers? What is the interplay there? Cybersecurity is a big deal. I'm assuming if you're up to some standards, you can get insurance.

ERIC: When I worked at a company a while ago, we were deeply connected with the insurance companies because we were incident response-based. That means most of our leads would come from Aon, Willis Towers Watson, Chubb, and Beazley. All of the big ones. Cybersecurity insurance is really interesting because historically speaking, it really only covered ransomware breach response, forensic analysis, and PR response. And a lot of these insurance providers are now starting to scale back.

What I've seen is you can typically get a policy or reinsurance policy specific to a control or operating environment. In a company that I used to work at, one of the things they were not able to do is get insurance for slashing and for staking of nodes. The biggest thing they we're focused on is ensuring that if a customer was to get slashed, which means if their node was to get penalized for either double signing or doing something malicious, they will be able to cover whatever funds were lost from that event with it.

What I'm trying to say is that there is no clear path forward based on what I've seen. And that's because they don't know how to necessarily monetize it. I think you're seeing insurance for custodial providers of up to X amount of funds based on what they have as assets under management. But that's still going to continue to change because I think Gemini and Coinbase are really the only two that have implemented it.

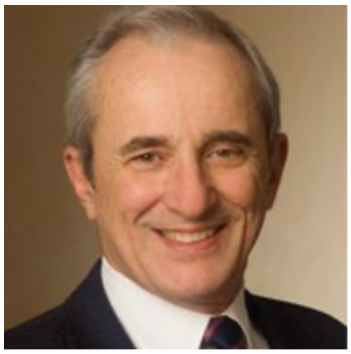
I think what I would see sooner is FDIC insurance for centralized and regulated exchanges becoming something more realistic than a very clear set of insurance policies. That's because these insurance companies are losing a ton of money on selling these policies, especially around ransomware. I think two of the five providers I mentioned earlier have already got rid of the ransomware policies because they were just losing a lot of money on it.

I bring this up because there is no clear path forward yet. And I think we're still waiting to see how the government shakes us out when it comes to regulated versus non-regulated. I think that will dictate what we will see around FDIC insurance for exchanges. And for those exchanges, I think they're going to largely cap or classify most things as a security with the exception of Bitcoin. I do think the law is going to be very clear in calling Ethereum a security, which is going to be a very interesting play.

But when it comes to insurance, I haven't necessarily seen a great policy myself. I still think that there is wiggle room. I've seen a lot of people work with reinsurance providers. Three of my old customers have worked with Swiss Re and Munich Reinsurance to get a better policy for what they wanted for assets and funds under management.

Thank you for downloading this DiffuseTap event transcript.

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

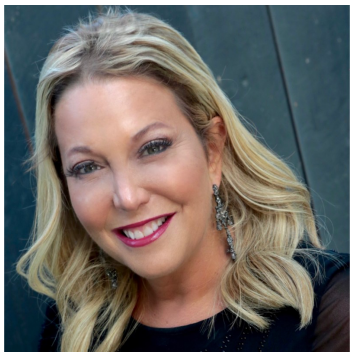


Dennis Chookaszian

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