diffuse*tap*
Virtual Event Series

Not Your Keys, Not Your Crypto

Guest Speaker:

Max Sherwood
Growth Manager
Unstoppable Finance

Hosts:

Kenny Estes
CEO & Founder
Diffuse

Ayla Kremb
COO & Co-Founder
Diffuse

DiffuseTap: Not Your Keys, Not Your Crypto

Last time on DiffuseTap, **Max Sherwood, Growth Manager of Ultimate Money,** talked to us about the FTX issue and what led to it, self custody and how users can avoid losing access to their assets, and whether crypto's mantra, "Not Your Keys, Not Your Crypto", is truly dead.

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

MAX SHERWOOD is a longtime Bitcoin investor. In 2019, he created Wholegrain Crypto, a platform where aspiring Bitcoin investors can enter the space with confidence. Soon after, he doubled down on the crypto market and took on a business development role at Finoa, Europe's leading digital asset custodian. Max is currently the Growth Manager of Ultimate Money

LinkedIn: @max-sherwood

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: Today, you're here to hear from Mr. Max Sherwood. Max, you've been here before. Would you mind introducing yourself a little bit and telling us about your background and what you're up to?

MAX SHERWOOD: Of course, Kenny. Glad to be back. Hi, everybody. I'm Max. I'm based here in Berlin. I'm a growth manager for Ultimate Money. We have built a mobile wallet app that is a self custody wallet, meaning it's your keys, your coins. I sometimes half jokingly call it the first decent mobile wallet, especially when it comes to DeFi because when I ask people, "what's your favorite mobile crypto wallet?", usually, no one has a ready answer to that question.

Crypto has mainly been a desktop-based activity, especially when it comes to DeFi. I'm sure many of you have experienced the joy of navigating DeFi with Metamask, which is pretty much what everyone uses at this point.

Ultimate Money has a team of people who have built, especially here in Europe, some of the leading FinTech and new banking applications. That includes Trade Republic, Revolut, whose equivalent in the US would be something like Robinhood, and others. It's going to be that kind of user experience, but it's a blockchain native experience. We're not holding your assets. We don't hold your keys. And especially today, in the wake of the whole FTX thing. I think this is a super relevant topic. Happy to be here, although it's kind of a sad day.

KENNY: Yeah. Because you mentioned that, let's go straight down the rabbit hole. Max, what happened? For the people who aren't aware of what happened with FTX and Binance, let us know.

MAX: Yeah. I'll try and do the short version, which involves FTX and its sister company Alameda, which is a trading firm. FTX is the exchange, and Alameda is the market maker. It seems that FTX was a bit too friendly and was giving Alameda some loans, but the collateral may not have been as good as it should have been. CZ from Binance was a big holder of that collateral. So is the FTT token, which is FTX' own token.

CZ basically came out and said that he was going to sell his massive position on this token. It started dropping in price, and I guess that was all it took to put FTX' solvency into question. Currently, I think if you try and withdraw your funds from FTX, you're just told that the withdrawal is pending. It's very much unclear what the financial health of FTX is.

Binance has already kind of signed it. I don't remember exactly what it is, whether it's a letter of intent or something, to acquire FTX, which would have been completely unimaginable eight hours ago. (Editor's note: Binance backed out shortly after this.) FTX has been a very profitable company, a great product. I personally have a lot of crypto assets on there, which are kind of stuck in limbo now. So, I'm qualified to complain from that point of view.

So yes, it's not not a great time. It obviously has affected the markets as well. I've seen some good discussions in the Diffuse telegram group here. I think I'll just leave it there.

AYLA KREMB: Awesome. Thank you. That was a very thorough and complete introduction to what's happened. I'll toss you into the other side of things, which is more around "not your keys, not your crypto". I guess that problem was emphasized with the news around FTX. Can you define what that really means? What does that phrase stand for in your world?

MAX: The keys are private keys. Most of the crypto runs on public-private key cryptography, where you get a public key, which is like your address. You can share this with other people to make yourself known, but you hold the private key. Whoever holds the private key can sign transactions and send assets around that are associated with that wallet or that address. "Your keys, your coins" is a very old, I guess we could call it a rally cry.

It's a piece of crypto history that has been repeated since the very early days, especially among the old Bitcoin community. Everyone was very much advocating for self custody, holding your own keys, and being the only one to have control over your assets. That's what we call self custody. I wouldn't say it has lost its importance, but it's something that we don't hear so much anymore in recent years, as we've had better and better centralized custodial service providers, like FTX.

I think people started to feel pretty safe, myself included, about leaving assets on exchanges and custodians. In May, we saw Celsius and Voyager and all of these centralized companies blow up. And for a lot of people, their assets were suspended in limbo. And now, we're seeing the same thing happening again with FTX. So I think "Your keys, your coins" is once again a piece of wisdom that we should have all paid better attention to.

KENNY: Alright. Let's say I'm new to crypto, and I like the prices because I think it's a good buying opportunity, depending on how you view these things. What are my options if I want to get into crypto? You mentioned Metamask. You mentioned exchanges. How can I go about buying crypto? What's a safe way to do that, and what are some of the pros and cons of the various options?

MAX: Generally speaking, there's a self custody option, where you probably are going to get a seed phrase, you're going to get your private key, and you're going to be responsible for storing it. Usually, you write it down on a piece of paper, or maybe use some other backup option. Or, you can make an account on Coinbase, FTX, or a custodian that specializes in holding private keys, and you can on-ramp there and have your crypto experience there. You can also do a mixture of both.

On the self custody front, the thing that most people think of is a hardware wallet, like a ledger wallet, which is one step better than a hot wallet. You can have a wallet on your computer, but it may not be as secure as a cold wallet, which is a hardware wallet. On the service provider front, there are decent

custodians out there. I actually used to work at a custodian here in Berlin called Finoa, and there are various levels of regulation and standards built into that space as well.

There are a lot of options out there, but I think self custody is still a user experience that has a long way to go before it's something that's very easy, and doesn't create the risk of the user losing their own keys, which is probably a lot more likely to happen then someone actually hacking your wallet

AYLA: Absolutely. Another question that might be interesting to look at is the concept of a wrench hack. Most people put their seed phrase on a tiny piece of paper, and they might pop it into a safe. Is that the best way to go about it? It feels like this is a weak strategy. Assuming that you don't want to use a centralized service, is there a better way to keep track of your seed phrase?

MAX: This is a real problem. The $5 wrench attack is, you go out, you buy a wrench for $5, and then you basically show up at the person's house and demand them to give you their private key. It's the lowest level of attack that you could do, but it's very much a real thing. Obviously, if you're keeping your private key at your house, there's all kinds of bad things that could happen, including your house burning down.

When we talk about self custody, it sometimes becomes a physical security problem. Your private key becomes a physical object in the real world that you need to keep safe. You need to make sure that it doesn't catch on fire, doesn't get stolen from you, your dog doesn't eat it, or whatever. Maybe I can talk about our approach at Ultimate right now.

The first step when you go into the Ultimate wallet is you get a seed phrase that, obviously, you can write down on paper, but you also get the option to encrypt it and back it up to Apple iCloud, which is a fairly basic option. A lot of people in crypto look at us weird and ask why we do that, but we've read that 95% of Apple iCloud accounts are 2FA encrypted, so that's pretty good.

Also, it's a retail wallet. It's not meant to have millions of dollars of assets going through it. We're probably moving past the day and age where people are keeping their seed phrases on pieces of paper. We're moving towards solutions built on Apple iCloud, or some other competitors. Google Drive is a piece of this. There's also a more sophisticated key sharding technology where I can hold a key, my lawyer can hold a key, and my friend can hold a key. The three of us need to come together to restore my key if I lose it. There's a lot of options out there.

But yes, I think it's not always the best option just to keep your seed phrase on a piece of paper in your house, or even on a hardware wallet in your house, or something like that. Unfortunately, there is no silver bullet for this kind of problem. Custody is a problem that has always existed in crypto, and we've come a long way. But some of those basic challenges are always going to be part of being your own bank. You're going to have to take security and custody seriously.

KENNY: You mentioned being your own bank, which segues nicely into a favorite topic around these crypto discussions: regulators. How do they enter into this? Is there a lot of clarity there? Because candidly, having to split it between your lawyer, your accountant, and your wife doesn't seem like the best solution. Is there a regulatory landscape or solution coming down the pipe that is going to make it a lot better for everybody? What do you see in the future there?

MAX: This is a big topic to unpack. I think when it comes to custody, first thing's first. Creating a public-private key pair is just math. It's something that we've been able to do with cryptography for decades already, and it's not something that you should ever try and prevent any other human from doing. That's just my opinion. You can't directly regulate or enforce any behaviors when it comes to creating private keys.

I think people should always be able to create a crypto account and a private key. In terms of regulating custody, I think there definitely can and should be regulation on the custodial front. Here in Germany, there is such a thing as a custody license from the financial regulator, which says that you meet a certain standard as a business that other banks and other financial institutions have also met.

That's well and good because if you're a hedge fund looking for a custodial provider, when you see that they're regulated in Germany, you can have confidence in that. But yes, I don't think there's much for the regulator to do when it comes to self-custody. A wallet builder like us, we pretty much exist outside of any real regulation.

We've had hiccups related to the DeFi stuff that we do. But in terms of self custody, I think that always should be something that's left to the individual. I don't think that's something that should ever be touched by regulators directly.

AYLA: I have one other question around "your keys, your crypto". Where do you see this actually going? The reality is, the reason we have banks today is because people don't like keeping their money under their mattress. Not everybody is ready to take that level of responsibility. Do you think there is going to be an emergence of more reliable centralized parties that we could potentially work with, who have completely transparent balance sheets where nothing is hidden? How do you imagine the future of this space?

MAX: Coming back to FTX, it looks so similar to what happened at Voyager, and by extension, Celsius, and Three Arrows. People were lending too much and creating too much leverage on top of customer funds. So when you see a balance of one Bitcoin on FTX, I guess what was really happening in the background was half of that Bitcoin was being lent to Alameda or something like that.

When you see balances on a centralized provider, you can't go on a block explorer and actually confirm that the balance is there. You also can't confirm that it's just your balance, that it's not being re-hypothecated and we're not just recreating fractional reserve banking in crypto. That's a problem.

You talked about transparency and balance sheets, and I think that's definitely something that should probably happen in terms of custodians, and probably also centralized exchanges, where they're going to have to prove to the regulator and prove to the customer that those funds are there, and they're not being lent out or existing in two places at once. I don't think any of us expected FTX to be doing this kind of thing.

But that's obviously not good enough. I can definitely see a future where there's more regulation coming down the pipe in terms of transparency for crypto businesses, and proving that the assets are there and that they're not lending them out or trying to use them for leverage in any way.

KENNY: I'm circling back to raise a question here from the chat. It seems like the industry is getting more comfortable with MPC-type solutions, or at least multisig. You mentioned that FireBlocks, Copper, and Anchorage here in the States are also federal custodians that have an MPC type solution. Do you see that being the way forward, where you can verify your balances anytime, and you can make sure that they're your own and there's interoperability between them? Or do you think that fundamentally, that is still going to have the hack risk, and there's weaknesses attached to it?

MAX: So we're talking about MPC versus standard one key, one account?

KENNY: Just generally custodians that have an MPC solution as being the centralized holders of capital and keys on a go-forward basis.

MAX: So, I worked at Finoa, which was a hardware security module-based solution. MPC is multi-party computation, which has more to do with key shards and two or three, or three or five setups. I even wrote a piece on their blog explaining that they're not necessarily in competition with one another. They're just orthogonal to each other. They serve different purposes for different people.

It might be a little bit into the weeds, but I guess I can talk about what is on the retail front, which are smart contract wallets. These are wallets that are actual smart contracts. With these, you don't hold a private key in the same way as you used to before. Ultimate is kind of an old fashioned, externally owned account wallet, where you get one private key and you basically have one account.

The whole Ethereum community is already resoundingly saying, "Oh, smart contract wallets are the future of adoption, because they unlock more features. " My problem when I hear the Ethereum community presenting this new technology is that it feels like developers building tools for developers.

So, when they talk about adoption, they expect everybody to have multiple hardware wallets, and multiple friends that are knowledgeable about crypto, who are willing to be your guardians.

They also talk about social recovery. Some of the more sophisticated technologies like MPC or smart contract wallets can allow for social recovery or something that resembles them in multisig. But I don't think that more sophisticated technology always renders a better solution for the user, or a better user experience. That's why Ultimate just decided to go with a seed phrase and an iCloud backup, which is pretty controversial in the space. But I think in terms of the experience that it creates for the user, it's actually very simple. They're not likely to get turned off by complexity.

And also, they're less likely to lose their key, which I think is the real problem that all of us are worried about. We're less worried about some sophisticated actor hacking your account. We're pretty much worried about the user losing their private key, which happens way more often than actual theft. I hope that answers the question.

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