Transcript: Anchorage: Crypto Custody Reimagined

Featuring: Diogo Monica and Ash Bennington

Published Date: January 12th, 2020

Length: 00:49:10

Synopsis: Diogo Monica, co-founder & president of Anchorage, joins Real Vision senior editor Ash Bennington to discuss Anchorage, the growing institutional interest in crypto, and the evolving regulatory environment. Monica shares his background in academia, highlighting his studies in computer science and distributed systems, well before he got into the crypto space. As institutional investors are increasingly looking to gain exposure to crypto, he explains the importance of key management to institutions. In order to meaningfully invest in crypto, they are required to meet the highest level of security standards—specifically, they seek key management that doesn't depend on any single individual for the security of the assets. Monica also points out the difficulty for regulators to stay on top of the crypto space due to the rapid pace of development, but that companies such as Anchorage are working closely with them to ensure compliance for users. Filmed on January 7, 2021. Key Learnings: Many large institutional investors are looking to break into the crypto investment world, but are holding back because of the lack of security and regulatory uncertainty among platforms. Solving the key management and custody problems institutional investors face will enable many of them to enter the crypto market. Not only should this add more investment liquidity to the space, but those that solve this problem should benefit from being the institutional gateway.

Video Link:

https://www.realvision.com/shows/the-interview-crypto/videos/anchorage-crypto-custody-reimagined

ASH BENNINGTON: Diogo, Welcome to Real Vision.

DIOGO MONICA: Thank you so much for having me. It's a pleasure to have you here.

ASH BENNINGTON: Diogo, tell us a little bit about your background. You have a really interesting background on the tech side before you even transitioned into crypto. Tell us a little bit about what you were doing before you jumped into crypto.

DIOGO MONICA: Yeah, it's been quite the journey. I would say that my career started in the academic realm. So I did a PhD, a master's, and a bachelor's in computer science. And during my PhD, I actually worked on distributed systems issues that at the time, I didn't know, but 10 years later, 14 years later, actually super relevant for blockchain. I was publishing academic papers and hash cash, business Byzantine fault tolerance, distributed randomness, that were just academic pursuits at the time, and not at all applied to monetary policy, but that turns out are actually useful 14 years later for the crypto space.

And so I went from a PhD to being an early employee in a company called Square, where I led the platform security team, one of my claim to fames is that I actually– or claims to fame is that I was actually part of the team that created the first encrypted credit card reader. And so we're on the patent for that, and we're able to do all the security aspects that safeguard all of the credit card transactions at Square– to this day, still does.

And the interest in crypto really came from the fact that I already had all the fundamental underpinnings from an economic perspective. And so in 2013 when Bitcoin started becoming popular, and I saw what the underpinnings of the way that we're solving the Sybil attack, and the way that Satoshi Nakamoto had decided to solve that specific problem, I was immediately interested. Not necessarily in the investment side of the interest, unfortunately, but more interest in the academic sense of participation, and just playing with the technology.

And then from Square, I ended up joining Docker and I was a security lead AT Docker. And then the idea from Anchorage came from the work that both myself and my now co-founder, Nathan McCauley, did for all those 10 years, because we actually joined Square the same week 10 years ago. And so we went together from Square to Docker, and then a lot of people are reaching out to us for help with crypto custody.

And they were investing funds, that are investing in these new crypto assets, and did not know how to do security for them. Did not know how to do operational security. And so they were asking us for help. So that's kind of how Anchorage came to be.

ASH BENNINGTON: Yeah, it's extraordinary. One of the things that keeps coming up in these interviews is when you look back on your life, you see an order that you didn't necessarily see looking forward. But the points that you made, the things that you were interested aren't just relevant to crypto, they are crypto. It's the very core of what makes crypto crypto.

DIOGO MONICA: Yes, that's absolutely right. In fact, from a security researcher component, it's a little bit sad that crypto now means cryptocurrencies, not cryptography how it used to mean 14 years ago. I'm not sure– I'm split torn on that debate. But yes, you're absolutely right– it really was the academic interest and the underlying technology that got me interested in the crypto assets themselves. And it was the background in private key management. I worked on private management at Square. I worked on private management at Docker.

And then ultimately, the way that Anchorage started as custody platform, which now is really the whole platform that does a lot more than custody. We obviously do brokerage, and we do financing, lending. We have a full suite of services. But at the time, the core technology that needed to be built was at its essence private key management. Private key management of billions of irrecoverable cryptocurrency.

ASH BENNINGTON: Yeah, and I'm sure we're going to go down the rabbit hole into some of the academic interests you had a little bit later in the interview. But to come back to Anchorage, the core offerings that you have– tell us a little bit about when you spun up the company, what was the core problem that you were trying to solve?

DIOGO MONICA: Anchorage started in 2017. The main problem that we were trying to solve was that there was no technology for institutions to use if they wanted to have hundreds of millions or billions of safe crypto asset investments in a way that was regulated and that met the highest standard for security. In fact, at the time, and still even today if you look around, the best-in-breed technology for protecting digital assets, the most sophisticated digital asset that we had ever come up with, is essentially the same technology that pirates used in the 1700s to protect their gold coins.

Three years ago, it was pirates burying their gold in a treasure chest, and finding an island somewhere, putting a treasure map on how to find it, and that was the technology in the 1700s. And three years ago, what institutions had available was cold storage, which was the equivalent. It was USB keys or smart cards in safety deposit boxes in buried mountains somewhere, and checklists that they should follow to actually recover the assets.

Obviously, that does not work for institutions. You cannot build a product or service– and even as an investor, you cannot be two whole days away from your assets if you want to have liquidity, if you want to participate with them. And then the moment Bitcoin became not the only game in town, and Ethereum came to play, and all these DeFi building blocks– those are all private key interactions. You require the private key that owns the assets to participate with them. And therefore, investors cannot be locked away with their assets in a mountain. They need something better. So Anchorage was created with the sole purpose of creating a security solution that was digital in nature and as sophisticated as Bitcoin itself.

ASH BENNINGTON: Yeah, so in many ways, the problem that is the glory and the challenge of cryptocurrency at the same time. And it really is a fascinating space. So tell us a little bit about what your key insight was that let you think that you might have a real business here.

DIOGO MONICA: I think the key insight was just 12 years of experience in key management in building systems that moved hundreds of billions of per year at scale successfully. And so the insight was, hey, I understand what the instinct is. People are solving digital security by resorting to physical guarantees and physical security. The instinct is to put something buried in your backyard, put it under your mattress, or solve it with armed guards. We know how to do that. We've been doing that for gold for millennia. And so we know how to do that very easily.

And there was no technology that was purposefully made for protecting private keys that were digital in nature, and that stored hundreds of millions or billions of dollars. And we had built technology that was very similar for different sets of problems around private key infrastructure, and around key distribution, so we knew how to use systems like hardware security modules. We knew how to actually run business logic and hardware. We knew how to do biometric authentication of users. We knew how to have no single points of failure in your systems and in your humans so that no individual can actually steal the assets of an organization.

And we obviously had a lot of these insights and a lot of clients coming to us that we were helping when we decided to actually start Anchorage and to build the platform to onboard all of them into it. And so the insights really came from our experience. I think the best way that I like to describe this is somehow, we were handed in a silver platter, the perfect Venn diagram of our skill set– academic experience in distributed systems, security in a financial infrastructure moving hundreds of billions of dollars, and operational security, and infrastructure security at Docker. And the Venn diagram is literally private keys that are worth billions of dollars. There's not that many things that I'm good at, but this one thing was particularly perfect for us to go out and build the company around.

ASH BENNINGTON: Yeah. So unpack that for us. Take us through the next level of detail about how you think about the nature of the problem and distributed systems around key management, and what the solutions that you've developed is specifically.

DIOGO MONICA: Absolutely. I think there's three main components. And everyone that talks about cryptocurrency security usually only focuses on one. So the three main aspects that I like to think about are private key generation and safekeeping. So the main issue that people solve, the cold storage. But the other two issues are user authentication– how do you know that this person is who they say they are.

And the other issue is patterns. Is this the pattern of behavior of this human, and is this pattern of behavior of the organization itself? So those are the three problems that need to be solved. There's many, many, many, many other ones, but these are the three largest problems that need to be solved for you to have a platform that can have crypto assets in a safe manner.

And so if I dig deeper into them, the way that we solve them is on the private key generation and safekeeping, we make heavy use of hardware security modules, which are these pieces of hardware that were explicitly created for the purpose of key management. But we actually go further. And we put the code, the logic, the policy engine that tells that Ash is authorized, and Diogo is authorized, and Diogo and Ash have to collaborate for this transaction to go through–

that's actually encoded into the hardware alongside the key. There's a lot of issues when people put the policy away from the private material, but we've encoded around it. We've surrounded the key with a policy. And that solves the first layer.

The second layer is how do you authenticate the humans. And so we make heavy use of biometrics, several types of biometrics to understand if you who you say you are. And obviously, private keys and hardware also on the client side to ensure that the devices are not compromised.

And then the third component is all the data that we collect around the pattern of usage of the organization and of the individual. So for every transaction or action, we know if the organization usually does it, and if this human is one of the ones that participates in this type of transaction approval. So all those three are the building blocks or the pillars of a system that allows you to go and have safe custody for billions of dollars.

And not just custody, because custody is easy. The problem is when you try to sell the assets, move the assets, participate in the assets, participate in DeFi and governance protocols. How do you do that if you buried your assets in a mountain somewhere? The answer is you can't.

ASH BENNINGTON: That's so interesting. Custody is easy– that's such an interesting way of framing it. But it's everything else that's hard around it. Let's go through those one at a time. I'm really interested to talk about the key generation safekeeping point. Very often, the question gets asked, I hear a conversation that goes something like this– well, how do you do that? Oh, it's a dedicated hardware module. And that's generally where the conversation stops. I don't really know much about the state of play currently in hardware security. Talk a little bit about what that is for people who may not know about it except that it exists.

DIOGO MONICA: So hardware security means lots of things. There's several types of hardware security or pieces of hardware security. The ones that we use our hardware security modules, which are effectively pieces of hardware that are made for not only private operations, but they have physical security properties. So what I mean is a lot of them have anti-temper temper detection and temper protection mechanisms. So if you tried to drill into them, they wipe themselves out. If it gets too warm, they wipe themselves out. If you try to do power analysis, it wipes themselves out. So they're purposefully built for people to not be able to extract any secrets out of them.

But they're only really one type of hardware. There's many other types of hardware that allow you to generate private keys in a safe manner. And all of them have different security focuses and definitely different price points and different trade offs.

Another one is enclaves. People talk a lot about SGX on the Intel processor, and the ability of generating inside of those enclaves, private keys. That's another way that you can do private key generation. And then finally, you obviously have other mechanisms of private key generation in other types of hardware. Sometimes, people use just an offline laptop– as simple as just a normal laptop that is offline. And that would also be one mechanism for you to try to do private key generation.

One of the most important things here is the code. What code are using for the key generation, how audited is it. And the second most important thing is randomness. Where is the randomness coming from? How do you actually know that you're generating random private keys and that the random number generator is not biased? So all of those things are things that you have to deeply care about. Some of them have software solutions, some of them have hardware solutions.

But by and large, they use of hardware security modules has been in vogue for 25 years, 30 years, because it's what military uses for their communications. It's probably what's being used for a nuclear launch codes. These are the ultimate pieces of hardware that were created to protect our deepest, darkest, most dangerous secrets.

ASH BENNINGTON: Yeah, that's so fascinating. I'm curious, to move on to the next level to talk a little bit about biometrics– I think that's something that obviously, everyone who has a smartphone has some experience with– but I'm curious about how the specific applications around private key management are implemented.

DIOGO MONICA: Yeah, so think about someone that has claimed that it's protected, generated correctly the key, protected the key. Usually, it stops there. There is no known mechanism or good mechanism to identify the humans that are making the requests to move bitcoin, for example. You want to move bitcoin, sure, you've protected the private key, but who is actually requesting that, and are they authorized? So there's a lot of solutions out there, of course. And one of the solutions sometimes is a dedicated piece of hardware, say a YubiKey, where people are clicking the YubiKey, and the YubiKey actually allows them to sign some transaction and be able to go through with them.

But if you think about it, there's actually several problems with that. Even for the people that do that, they have several problems with that. The first problem is you don't actually know what you're signing. When you're clicking the YubiKey, you know that there's an operation, but you don't know if you're sending 100 bitcoin or 10,000 bitcoin.

ASH BENNINGTON: Right.

DIOGO MONICA: The second problem is you don't actually know who's touching the YubiKey, because the YubiKey only has, effectively, a conducive layer. So when you touch it, it engages in operates, but it doesn't have to be me. It could be anyone. Sometimes, you even by accident actually touch them. And so those are problems that are real for crypto assets because of the scrutiny and because of the potential target of hundreds of millions of dollars that these keys hold. And so you need a lot better than that.

Number one, you need the ability to trust the transaction that you're seeing and audit it. Number two, you need the ability for the hardware to prove that you who you say you are. And so that's where the biometric authentication comes in. And number three, you need to not be able to do any kind of sensitive operation by yourself. You need these operations to be multiparty operations or quorum operations. So a two out of three, a three out of five, however you want to configure it. So those are the three main issues that you want to solve and that want to focus on.

And then on the subtype of biometric, just one type of biometric is not enough. So is not enough for you just to do face ID. So we layer in many types of biometrics and we learn as people go through the approvals process through Anchorage. And every time they engage with Anchorage, we learn more. Not just about their own biometrics and about their own authentication that changes across time, of course, but also, for the third point, which is their behavior, which is equally important.

ASH BENNINGTON: Yeah. And that brings us to the third point, which is the pattern recognition component. Understanding what typical usage patterns look like, what atypical usage patterns look like. This, is probably the one that we hear the least about. Tell us a little bit about what the philosophy is that drives Anchorage in this space.

DIOGO MONICA: Think about different clients. Different clients have different profiles. Some of them are heavy traders. They're daily traders, they're trading, they use our brokerage APIs to get the best prices from the market, and they're constantly in and out of positions using our APIs for settlement. And that's a very different client and a very different type of operation than, say, a crypto fund that is invested in an asset, and it's going to sit on that asset for seven years.

These are two very different types of behavior. But not just that– they also have very different types of policies that should be enforced. And so think of a trading team. Usually, they're primarily in the same office, the same location. They're usually close to one another, and they have these bots or these APIs they are actually using doing the trading, but they're coming from one location, one office. But it's very frequent that a VC fund or a crypto fund owner is actually traveling, going to conferences– at least they were before COVID hit– and approving transactions from anywhere in the world. Another very distinct pattern of behavior.

Our technology allows us to adapt to the different type of client and tell our risk engines if this is a transaction that should have further scrutiny or that should be approved. And then we've made the technology in such a usable way that it really is a pleasure to use it, and it's very easy for us to collect further information if we're in doubt. So it is so easy for you to get an approval of three out of five people that if one of the people now is all of a sudden in a couple of hours, approving a transaction from Mexico, it's suspicious because they actually lived in Seattle. So that's very suspicious that an hour later they were in Mexico doing a transaction so it's very easy for us to request further approval and authorization from somebody else in the quorum.

So it's not just that we have the data. It's not just that we fit into the profile of the specifics of type of clients. It is also that we've created such a usable system that allows us to have a level of security that nobody really can get without at least putting a lot of hoops in between our clients and their assets.

ASH BENNINGTON: So talking of clients, tell us a little bit about your market positioning. This is an institutional product. Tell us a little bit about how you work with clients and what that transaction typically looks like.

DIOGO MONICA: We are an institutional platform that allows people to build products in crypto. So we have not only the infrastructure layer– so the APIs for custody, the API for brokerage, the APIs for you to build your products on top like pricing, so on and so forth. But you have the prime services that allow you to do those. So we can buy and sell, we can lend, we have financing, we have a partnership with Silvergate where you can actually have US dollar loans collateralized by Bitcoin. So that's the second component on top of the infrastructure of the prime services.

And finally, everything is wrapped with the regulatory scrutiny, audits, SOC 1 by EY, insurance– all of these other aspects that large institutions want. So you're absolutely right that institution is our prime focus. The goal of Anchorage is to be the institutional platform for cryptocurrencies, and allow all of these new banks that are coming out, neo banks, challenger banks that want to come and compete with Paypal, and that have seen Square and PayPal add these products to their Square Cash, into Venmo, buy and sell a bitcoin. They want to do the same.

ASH BENNINGTON: Talking of institutional clients and customers, I was having a conversation on a podcast with one of the smartest guys, I think one of the deepest thinkers in the space, Ari Paul, and we were talking about the nature of adversarial thinking, and how he thinks about this. And into the interview, he said, this reminds me of Anchorage. These guys are the smartest guys in space in thinking about this, and that's why we work with them, and that's why we invest in them. And i said, actually, I'm interviewing Diogo next week.

And so it's really interesting to see how there's this confluence of people who are having these sort of similar ideas, because you start to see what that gap is, what the needs are. And it's interesting to hear you basically start out with a custody product, and then you evolved all of these other solutions, because presumably, you have those relationships with the clients, you begin to anticipate what the needs are. I'm curious about what you think that says about the space, and where it's going, and what you see your business evolving into.

DIOGO MONICA: Well, let's talk about Ari. Let me tell you that there are very few clients that want to and have the ability to go in as much depth as Ari went to with our systems.

ASH BENNINGTON: I doubt that at all.

DIOGO MONICA: He became a client and then he became an investor after he'd seen it. The type of extreme measures that Ari was doing for self custody before he moved to Anchorage were worthy of note. They were worthy of being talked about, because they were very extreme in nature. And I think to answer your question directly, people like Ari Paul that take everything seriously, they take the investment thesis seriously, they take the hiring of the collaborator seriously, and they take the custody, and their fiduciary obligations very seriously, are moving to platforms like Anchorage, and are moving to Anchorage, which actually allows them to just focus on their business, because they know that everything else is taken care of.

Things like the fact that you can buy and sell through Anchorage from the safety of the Anchorage custody platform immediately remove a lot of the issues, allow you to actually be faster at executing your trades. We give you the best price, because we actually go out to source multiple

liquidity providers. And so these were the things that were not available two years ago, three years ago, and that really kept institutions in the sideline. And now you see this new wave in the Bitcoin prices and the crypto assets prices going up. And I believe part of the reason is– not I believe– I know for a fact that part of the reason is because platforms like Anchorage exist today, and did not exist three years ago.

ASH BENNINGTON: Yeah, it's also so interesting to think about how the crypto space is evolving. The things that you've mentioned, things like NBBO, National Best Bid Best Offer, Reg NMS, things that have existed on the traditional capital market side of the equation for many years now, just coming and spinning up in the crypto space. Until very recently, there were these huge deltas between exchanges that you would get. I'm curious now to hear that's now part of your business, as well. Tell us a little bit about that.

DIOGO MONICA: A lot of the road map of Anchorage has come from client interest. The same way that we don't believe that the platform should dictate the investment strategy, and we support hundreds of crypto assets, we also believe that we are following the client's demand. And it was really interesting, because when Anchorage started, primarily, we were a regulated custody platform– that was the primary product that we had, was custody.

But then it was immediately obvious that clients wanted to trade from the safety of Anchorage. They didn't want to go anywhere else. And so what we've built is dashboards that allow you to buy and sell, get bids, and an API for a lot of these traders that want to automate that to get effectively, RFQ. They get quotes and they get to accept quotes, and trade that way.

I think this is essentially one step closer to what traditional prime brokerages do in the traditional world. And I think the space in general is not quite there yet in terms of all of the bells and whistles and all the functionality. But we're very close. And work that is done from people like Anchorage, and integrating these products– not in segregated products– there's really no traditional players that are very big that only do execution. They're always bundled and some kind of vertically integrated prime brokerage. The same thing is true for crypto.

And you talked about brokerage, but it's very interesting, because all of these things are interconnected. We do financing. We allow you to get US dollars backed by crypto, backed by Bitcoin, in this case. And so you can actually do leverage. You can have hundreds million dollars of Bitcoin, and get a loan, and buy more Bitcoin, if you so desire. And so that's another thing that is absolutely trivial for you to do in the traditional world, but it was very hard for you to do two years ago at the institutional grade, at the institutional level with the amounts that institutions wanted, but that then pulls in lending as yet another one of the components that are needed to really complete the picture. So think about how Anchorage is trying to integrate, and all of the features of crypto, and the vertical integration of all the services of prime brokerage under a regulated institution that people can trust.

ASH BENNINGTON: You know, it's so fascinating– one of the things that I find most interesting about crypto is that it's a mash up of three different spaces. Very sophisticated computer science cryptography. Then you have very sophisticated financial analysis. Things that you're talking

about that would be traditionally within the structure of a prime brokerage agreement between a hedge fund and a bank, for example. And then the third component– very, very complex legal regulatory compliance elements. It's a lot to put together in a single stack or a suite of services.

DIOGO MONICA: It really is a lot. And I think that's where a team really matters. I think that was the main focus of Anchorage. It was not just safety from day one. And that being the core of our business proposition– is we're giving you the ability of participating in the crypto ecosystem, but with the safety that you're familiarized and familiar with from the traditional world, but really, the team in the execution.

I have to say that our legal team has been absolutely amazing. In fact, Anchorage is probably going to be one of the first, if not the first crypto companies in the United States to get an OCC charter, to actually be a Federal level bank. And so getting a charter from the FCC at the Federal level would be fantastic for the space. And we're very excited about those types of developments that bring further clarity on the regulatory realm of crypto assets in the United States.

And it just doesn't limit their impact in the United States, of course. It does have worldwide impact. But it's a recognition that there's very clear ways for people to get involved. And that's part of the reason why you're seeing so much excitement. There are so many banks coming to Anchorage right now. Neo banks, challenger banks, bulge bracket banks that want to participate, and need this technology, and need this custodian or this technology platform or these prime services stacks to offer services and businesses in crypto.

ASH BENNINGTON: Yeah, I'm so curious about this. Tell me about the current state of play in the legal regulatory compliance realm. Obviously, we're talking about SOC audits earlier, regulation by OCC. How is that space developing? How is it evolving? Do you find yourself in a position where you have to educate the regulators? Are they relatively sophisticated? Tell us a little bit about the state of play there.

DIOGO MONICA: It's changed dramatically. At this point, the regulators are very smart about the space. The regulators are very informed about the space. Three years ago, we were having a lot of earlier conversations around technology and guarantees of assets like Bitcoin– so in the early beginnings. And then things moved on to talk about forex, and what are the potential of forex and the difficulties of forex. And then we moved on to talk about potential issues downstream, and denial-of-service, and when assets are available and not available.

And then we moved on to start talking about other types of blockchains, other types of technologies. Then we started talking about staking. And then we started talking about DeFi and lending. So it really has come a long way. And I don't envy the position that regulators are in, because we see how fast this space is moving. And we see the massive amounts of money that is being put into these completely untested protocols.

The regulators have a huge important in the space and ensuring that there's no criminal activity, and that people can't shoot themselves in the foot too much. Or at least that only the sophisticated institutions that really know what they're doing get to participate, and they're protecting people.

And it's hard to obviously protect people when the space is moving just so fast, and everything is changing from one day to another. Think about three years ago and think about 2020, and the rise of yields farming and DeFi, and how crazy mind-boggling complexity it is to track all of these protocols interact with one another on top of a blockchain. It's just fascinating to see them pop up, but also very, very hard to keep up.

ASH BENNINGTON: Yeah, and the regulators have just a Sisyphean task in front of them, right? And being accommodative to the technology, letting the marketplace develop on its own, while simultaneously protecting consumers, ultimately, from bad actors, maintaining AML, KYC, stopping things like terrorist financing. It's a pretty complicated space that they were already dealing with, and then on top of that you layer in, what's the difference between a hard fork and a soft fork? And you kind of imagine– I picture these sort of very well-meaning folks in three piece suits– this is a big shift in terms of the head space that they're moving into.

DIOGO MONICA: Yeah, and one of the things, though, that I have to say is that companies like Anchorage and other players in the space have helped tremendously, and have really spent the time to make sure that all the resources that the regulators need are there. And show them how we do things, and really show them how high we can go. Because it's not really about lowering standards. In fact, when you talk about anti-money-laundering standards, there's ways for blockchains to have higher standards than we actually have in a traditional world.

Because of the way that some of these technologies are built together, there are ways for them to get things that they actually didn't have before, including many, many, many hops of transactions before the current transaction forever on an indelible ledger, publicly available for everybody to track. And so there are things like that they've obviously come to understand that the private sector really helped. And so I do think that they have a partnership of companies like Anchorage that are always available, and we have extremely good relationships with many, many regulators in the United States and internationally. And we are always the first ones to volunteer our own time to make sure that we understand everything that is happening, even on the bleeding edge.

ASH BENNINGTON: Something else that I've really wanted to ask you about, Diogo, is you're so uniquely positioned because of the conversations that you have with institutions– I'm curious what you're hearing and what you think the current landscape looks like in terms of people making this transition from the traditional capital market space into digital assets.

DIOGO MONICA: I think when we talk about institutions– institutions being so many things– when I say that we're an institutional platform, I really mean it in the largest sense possible. It could be sovereign wealth fund, it could be a VC firm, it could be a crypto fund, it could be a hedge fund that is trading actively. It could be a miner, it could be an exchange, it could be a neo bank, a challenger bank, a bulge bracket bank. There's all of these types of institutions. Really, the definition is you're not a natural person is at the end of the day, what the institution means.

ASH BENNINGTON: But let me jump in and ask. How do you think about that hierarchy? How do you think about that structure? When you think about institution, how do you classify those different organizations and what their needs are based on what they do?

DIOGO MONICA: I would say that there's maybe four large buckets. There are the people that are investors, and they're actually doing buy and Hold they're investing in an asset, they are speculative in nature, they believe in the protocols. They're buying and actually waiting around, some of them generating yields, some of them not. But by lending, we have a lending ability to lend out Bitcoin, for example, or could process and generate yield. So a lot of them are in that bucket, which is they are making an investment, and they're speculative in nature.

Then you have maybe institutions that are more crypto native, and want to build on the things that are available on the bleeding edge. They're creating a specific fund that takes advantage of taking yield. And so they have a specific need around owning this asset, and actively participating on the network, and doing smart contract execution and protocols. And they're interested in the financial instruments, but very much on the bleeding edge of trying to take advantage of everything that's happening.

Then you have institutions in crypto. So you have the exchanges, you have the miners. You have people that are trying to integrate and create new products or services for clients that are in crypto. And then you have the traditional corporate institutions of folks like PayPal and Square that they have normal businesses, but they want to add crypto to their portfolio. They see millennials being attached to this new type of asset and they want to get that relationship as early as possible, so they're adding this to their portfolio. But they're more traditional in nature, and they want to augment their current business capabilities. Those, I would say, would be the largest buckets that we have.

And of course, when you talk about investors you have anywhere from small family office all the way to sovereign wealth fund. And those are very different, of course, in scope. And the type of go to market sell is very different. The focus on compliance is very different. The focus on buy and sell, and how much slippage there is on a trade is very different for all these clients. And obviously, an exchange is very different from a miner, too, but by and large, these would be the large buckets that I would put them in.

ASH BENNINGTON: That's a lot of buckets and sub-buckets.

DIOGO MONICA: There is. And all of them have different go to markets. I think at the end of the day, if you look at Anchorage, you see that it ends up being the same sets of APIs, the same sets of platforms that give you the same sets of principles. Everybody needs safe custody. Everyone interacting with crypto needs safe custody. The majority of people need to buy and sell crypto, because they need to get into that position and exit that position at some point. So everyone needs a brokerage API.

And then the large majority of these clients benefit from having financing. From either generating more yield out of lending their crypto asset– like Filecoin is an asset that is very sought after, and has very high yield-generating capabilities from a lending perspective. Or just the ability of getting margin, and having US dollars backed by crypto in a way that they just couldn't get in a traditional bank.

And so it ends up being yes it's a lot of clients. Yes, it's different go-to-market approaches, but they all have the same basis. And so that's the beauty of this platform. The platform from Anchorage is integrated, has all these prem services, and everyone benefits every time we have a SOC 1– benefits everyone. Insurance benefits everyone. All of these security aspects benefit everyone. And then they have different use cases, but on the same platform.

ASH BENNINGTON: Obviously, it's been an extraordinary few months right now in the crypto space. It's Jan 7 as we're recording this, and I've got one eye right now on the upper right hand side of my screen, wondering whether Bitcoin is going to cross 40k when we're having this conversation. Look, obviously, prices gyrate, they go up and down. But the general trend here, the rise in price levels has sparked, obviously, a tremendous amount of interest in the space from institutions and individuals alike. I'm curious how you're thinking about that positioning more broadly speaking as the interest in crypto just continues to rise.

DIOGO MONICA: Look, the most important thing is not if prices are going up or going down. The most important thing is for prices to be right. For price discovery to be efficient and effective. And so that is actually the part of the play of Anchorage being here, and allowing liquidity, and allowing price discovery– is the thing that is going to bring institutions to the space.

Because volatility is exciting for some, not as exciting for others. What people don't want is come to a market that they believe might be influenced and might actually be influenced by actors that are trying to take advantage of the price swings and are manipulating the market. So market manipulation is something that a lot of these institutions no longer have a fear of in Bitcoin, but that was really one of the big questions two years ago, three years ago, when institutions were coming into play. They didn't know, they weren't comfortable with it.

So prices are going to go up, prices are going to go down. Over the long term, obviously, Anchorage is a big believer in the technology, and therefore, we are strong believers that many of these assets will be worth a lot more than they are today. But for the short term, what we need for prices is for prices to be right.

ASH BENNINGTON: So Diogo, as you think about the thesis, the importance of price being right, what are some of the things that you're going to look for as we go forward to make sure that this market is healthy and that think it is where it needs to be?

DIOGO MONICA: I think a lot of the aspects are supporting the features that these crypto assets have that are necessary for their good governance or for their liquidity. I think we're still very much in the early innings of the infrastructure catching up with the innovation of all these different protocols.

I think if you look at DeFi as an example, and if you look at yield farming, and Wi-Fi, and SushiSwap, and Uniswap, and all these different elements, these are very much outside of the reach of any institution. Institutions are now finally getting into crypto assets like Bitcoin potentially under the sort of value narrative. But these other really cool use cases and examples and building blocks that are being built are still out of the reach of institutions.

So there's a lot more value in crypto than the value that is currently available to them. And so part of our job and part of the mission of Anchorage is to expand what's available for them to not only invest in, but participate in.

ASH BENNINGTON: Yeah, it's one of the things that makes the space so interesting– is that there's always a leading edge of the curve that is ahead of where the mass of people are. And precisely as you point out, institutions obviously are not going to be using decentralized exchanges anytime soon at scale. It's interesting to think about that. How do you see that unfolding? Do you see an on ramp or an access path toward more decentralized protocols in the future that institutions will be able to access? Or is that something that for the time being at least, seems like it's going to be out of reach?

DIOGO MONICA: I think what we'll see is merging of all these books together in one way, shape, or form. So there will be entities that will merge the decentralized books in the centralized books in order to actually pull liquidity from multiple places. That will happen, invariably. If that will happen in the US, and if institutions in the US will have immediate access to it– obviously, the answer is they won't have immediate access to it.

But as time goes on, I am of the opinion and hope that we will find a way of continue meeting the very high bar that we currently have for KYC and AML, and the trust that institutions have when they come to a platform like Anchorage. And have that also pull in liquidity from decentralized financing, and these decentralized exchanges, because that would also be very beneficial for the space. More liquidity means better price discovery.

ASH BENNINGTON: Yeah, absolutely. All right, Diogo, I promise at the beginning of the interview that we'd geek out a little bit. I'm so interested to hear about your academic work, and how it's brought you to where you are today, and what some of the relevant issues are that you see in the space for Anchorage. Tell us a little bit about what you did and how you made that transition.

DIOGO MONICA: Yeah, so during my PhD, I was focusing on, well, two primary main areas. One of them was Byzantine full tolerant protocols. Solving the Sybil attack– actually, one of the biggest solutions that Satoshi Nakamoto presented was a way in a decentralized world, and a peer-to-peer world, to solve the Sybil attack by using proof of work.

ASH BENNINGTON: Tell us a little bit about what that means and what the constraints of that problem are.

DIOGO MONICA: Yeah, so the idea is that you have a set of identities, and you think about ideas these participating in some network. So you go out to the internet, and you ask who's around, and then 1,000 people shout out their names. Now the question is, how many of these people are actually real, and how many of them are fake? And now you can ask me, what is the definition of real and fake?

And so that's where the beauty of these protocols come in. The beauty real and fake or, the distinction between real and fake can be based on your computational power. So you have the right to present as many identities as resources that you have. As many CPUs or as many hashes you can actually do per second in this case. And so that then gets tied to electricity, of course. Imagine everybody had the same algorithm to do a specific hash function, then if nobody is faster than anybody else, then electricity really is the thing that you end up spending. And now you've spent the resources. It's not computational power, it's electricity. Who has the most electricity gets the most chances to participate in the protocol and the most identities.

And the problem specifically that I was trying to solve is, how do you do this in a wireless ad hoc network. So imagine that you in a war-torn area. There's a war, you're in a war-torn area, there's no infrastructure, and you have to deploy this mesh network. So you're going to have all these access points, distribute them around, but you don't have time to preconfigure them. You just want them to come up, identify each other, and then start working really in packets, making decisions about routing and allowing you to have access to some of their networks, some internal network.

Now the question is, how do you stop a rogue malicious adversary from popping up one of your nodes, compromising it, and then pretending to be 1,000 nodes instead? And then winning all of the votes? Because if you're making a quorum system that is based on votes, in which 2/3 majority actually get to decide how the protocol evolves, if I get to generate as many identities as I can without you stopping me, how are you going to do this? How are you going to have integrity in the system?

And so this is part of the type of work that I was doing in the academic papers that I was publishing based on computational resource tests, which, by the way, was the name that I used. And proof of work is definitely a better marketing name. And [INAUDIBLE] resource tests were not picked up as fast as proof of work was.

But also, different ideas. For example, can you actually detect how many radios a device has? And can you have one identity per radio? So instead of electricity being the defining factor, the defining factor would actually be the number of radios that you have. And using some elements, physical properties of radio communication, the fact that it's hard to send and receive simultaneously, and the fact that you can't really send wireless communication to multiple channels at the same time unless you have multiple radios. So I could actually detect the number of identities are actually participating in the system, and then converge on a correct set of nodes that then I could actually use as a majority for the elections that the system had to go through. So that was one of the main aspects.

And then the other aspect was usable security. I did a lot of research on bot nets. I did a lot of research on passwords and safety of passwords, and better mechanisms of choosing passwords that are not these one character, uppercase, lowercase, question marks, and all sorts of different characters nonsense that has to be eight characters. And those are artificial, and they are known for actually creating worse passwords, because people end up reusing them. And so better ways to actually define what a good password is and what a good password is not. So usable security and then distributed systems where the two main components that I was focusing on.

ASH BENNINGTON: Yeah, that's really interesting, because it's really too extreme different ends of the continuum. On the one end, it's really hardcore computer science, and on the other hand, it's really hardcore human behavioral stuff, right? So you can have the most secure password in the world, but if you write it on a Post-it note, you stick it to your screen, it doesn't really do a whole lot of good. So it's interesting to see that basically spend that entire continuum.

DIOGO MONICA: Yeah, so there's a reason for that. When I started out on my master's and my PhD, I wanted to prove to myself that I could do the mathematical elements of it. The more computer science-y [INAUDIBLE] and prove lower bound convergence, and upper bound convergence. And I actually had the skill set and the toolbelt to publish academic papers that were more theoretical in nature. And so I did that.

And then as time goes on, if you look at security, you end up realizing that a lot of the security elements and the security professionals don't care that much about usability or their users. They believe that if a system is able to be secure in some set of configuration, it does not matter how hard that configuration is to achieve for them to believe that system is secure. So what that means is that when something goes wrong, they say, oh, the user forgot to enable this flag, or the user forgot to do x or do y. And somehow, they are victim blaming, and actually putting on the user the complexity of configuring everything right.

And of course, that's just something that is absolutely wrong. And surprisingly, it took a long time for the information security community to catch onto this. And really, only in the past five, six years if people actually started stopping this victim blaming aspect, and saying, no, no, no, no, no– safety, not just security. It should be safe. The main mode of operating something should be safe.

And so I do have a motto because of that, which is to make safe easy and insecure obvious. And that's kind of what Anchorage also follows in terms of security guidelines in terms of philosophy for security.

ASH BENNINGTON: Yeah, so it's a perfect system except for those pesky human users.

DIOGO MONICA: That's right. The human element is always the weakest one.

ASH BENNINGTON: I'm curious, now that we talked a little bit about the human element, tell us a little bit about– because it's pretty extraordinary– since you did this PhD work, even relatively recently, there's been tremendous advancements that have happened on the distributed ledger protocols that do things like proof of work. I'm curious about your view at least of the current state of play in that space.

DIOGO MONICA: I think in general, all the solutions that are coming out have merits and disadvantages. There's no perfect solution in computer science. There never was and there never will be. And so what I like is the fact that we're getting many different types of protocols, some based on one type of proof of work, some based on other types of proof of work. Some based on proof of space and time or proof of storage. Some based on proof of stake, some based on proof

of authority. And we're getting these networks to be worth billions of dollars, and therefore, have the attention of the world. And specifically, of the world that would benefit if something is wrongly implemented.

And so we're having this massive bug bounty on all of these different blockchains that are implemented with very different security primitives and distributed systems primitives, and we're putting them under stress. Under load stress, but also under security stress. Because if something is wrongly implemented, as I'm sure you've seen, the protocols get hacked, and money gets siphoned away.

And so I love this ability of having all of these different types of systems out there coexisting simultaneously, and being tested. And I think that's the only way of actually seeing what emerges out. I think it's very hard for me to sit in my office and whiteboard the perfect solution, and then implement it in reality. Pesky reality usually has a way of humbling you. And so this is actually the better way.

ASH BENNINGTON: You know, it's funny– that's actually the perfect transition to the final question I was going to ask you, which is, what's your outlook for what we're going to see in the new year and beyond in terms of the real world application of some of these ideas?

DIOGO MONICA: I hope that 2021 is the year where people realize that stable currencies and stable coins specifically, in all sorts of shapes and forms– you can talk about centralized stable currencies or more on the centralized aspect, something like a USDC or a completely decentralized stable coins like Dai or elements of kind of blockchains like DM, which is more of a proof of authority play– I really hope that 2021 is the year where we see that proliferating. Where we see the underbanked Indian bank being able to take advantage of this.

Because as we've seen, Bitcoin has a store of value narrative pretty much locked in. But for day to day use, the volatility doesn't encourage people to spend it. And so there are issues there that could be solved with stable currencies while still maintaining a lot of the self sovereign aspects of crypto, and the sovereign-resistant aspects of crypto. So if we get to have a stable currency that is deployed in some of these countries that have seizure of assets, and that have hyperinflation, and that people get to benefit, and leave poverty or maintain some of their assets without actually being inflated away, I think that would be fantastic. And with DM launching this year, with protocols like Celo already launched and making really good progress, with USCC becoming more and more used, Dai proving over and over again that it's a system that is robust and that is here to stay, I think we might actually get a chance of seeing that become real.

ASH BENNINGTON: You know, that dovetails perfectly with our earlier conversation about OCC and this week's headlines of OCC clearing federally chartered banks to issue stable coins.

DIOGO MONICA: That's exactly right. It's one of the exciting developments, and one that obviously we're very excited at Anchorage, because of our potential OCC charter that we've applied for.

ASH BENNINGTON: I should say issue payments in stable coin, not necessarily issuing the coins themselves. But it really is an incredible time to be involved in this space. Diogo, thank you so much for joining us. I hope we can do this again.

DIOGO MONICA: Thank you so much for having me.