Generation Infinity X Space - XX Network Updates.

Thu Feb 22, 2024 6:06PM UTC

SPEAKERS
Bernie Cardoso, Aaron Welwood, Rick Carback, Darren Moore, Ryan Solomon, Mário Yaksetig

Darren Moore 00:00
All right. So, yeah, I'll start off. And I guess we'll start off with Aaron. And I just want to know if can you tell us how you got into the XX Foundation and why you're interested in the XX Network?

Aaron Welwood 00:16
Yeah, absolutely, man. Thanks for having me. Of course. My name is Aaron Welwood, I'm a director with the XX Foundation. So yeah, I actually joined through a friend back in 2021. We'd been we'd been in crypto kind of helping each other out since 2017. And, Paul, if you're listening, shout out to you, man - thanks for introducing me to David Chaum and XX Network. Anyways, back at that time, I just started researching a lot about David Chaum. The history that goes back to like 70s 80s, and everything that he did - pretty easy to look up if you haven't - just google David Chaum.

Aaron Welwood 01:00
Anyways, yeah, so I got into it, back then they had a betanet running at the time, where they were building up a decentralised node network. And I just dove in, I really didn't know much about that I started learning about, yeah, just how to run the Linux operating system. And, you know, started getting into that and then started running a node. You know, it was, it was a pretty amazing process, the whole team that did all that was very thorough. So it made things quite easy. And it was just a great community. So yeah, basically, that was it, the beta net node running, you know, scheme that they had is what I got into, and then that turned into main net.

Aaron Welwood 01:49
So the network's now something like over 365 independent nodes running around the world. And I think last time we checked, it was like 65 countries, it's obviously changing all the time. But anyways, something like that. Anyways, I'm a bit of a go getter, I noticed that this was going on. So the founding team eventually reached out to their head of engineering, Ben Wenger actually, you know, asked me, you know, Hey, can I call you - he calls me up and yeah, just kind of one thing led to another, I got a job with them. I started helping out in the community more and more.

Aaron Welwood 02:30
And eventually, I (long story short), I ended up on what is called the XX Foundation now as a board director. And we work along side some of the most talented people in the world in the sphere of

cryptography and software engineering, technology, innovation, so on and so forth. So the XX foundation was set up by the initial founders of the XX Network, shortly after they did the main net launch. And this was, you know, to continue guiding the XX Network, along that path of increasing growth, global decentralisation, so on and so forth. So yeah, that's about it.

Darren Moore 03:08
It's funny, we're talking about Linux, I was about to throw out like this old laptop, but I installed Linux on it. And like, I'm hooked. I'm playing around with it. I'm like, what else can I do is like, you know, the old laptops actually, like running fine. It's, you know, oh, it's..

Aaron Welwood 03:26
Yeah, it's unreal. The amount of resources it takes to run like, you know, windows, not to knock on Windows. But yeah, it's crazy once you see what you can do with Linux. So...

Darren Moore 03:36
Yeah, I there's something called mint Linux, it's, I don't know, it's rather like it - it's pretty fun to just kind of kind of see what's what's available on Linux and how to go about doing stuff. But back to what we're talking about. What are you most excited about with privacy and the XX Network?

Aaron Welwood 03:59
Yeah, I'm, I'm excited about this year. You know, there's a lot to be excited about, as you know, you've got a bunch of panellists here to share on numerous things that we're doing. So I guess what I'm most excited about is the actual development path that we're on now. Anybody that follows the XX Network, we've gone through kind of different iterations along the way, and we've been through, you know, a bear market and come out the other side, and it looks like things are, are on their way up again.

Aaron Welwood 04:32
And so I'm just excited about our positioning in 2024. I don't want to get into the details, because we have a bunch of other panellists here to share that we'll be able to do a much better job. But really, it's just the continuation and innovation that we're expanding the XX Network technology, the community is growing, people are excited again. We have such a passionate community you know, If you if you've been in our telegram chat it gets, it gets pretty hot in there, in terms of people have a lot of high expectations, because if you understand the technology that undergirds our network, you realise how important this is.

Aaron Welwood 05:16
And it can be a lot of pressure in terms of we realise how important our privacy is online and how critical that is to society. And that really is a lot of responsibility for those of us that are part of this movement. So I'm really excited about this year, we have so many things lined up just our... back at the beginning of January, our team was going over: "What do we put in our Q1 roadmap?' and there was so many items, just in the first quarter that we actually had to leave some things out, which I was excited about that. I'm like, This is amazing. Like, we've got so much going on, and it's just the beginning of the year, people have no idea how awesome this year is going to be. So yeah, I hope, that people are strapped in because there's definitely a lot more to come. It's gonna be fun.

Darren Moore 06:15
So, do you think do you think people care more about privacy or less about privacy today?

Aaron Welwood 06:26
Well - they absolutely care about privacy. I mean, you lock your doors at night, right? You close your blinds, it's just I mean, it's really a matter of there's varying degrees on that, because it really depends on what an individual's understanding of what's at stake regarding their privacy, you know, in society and culture. You know, for us, obviously, it's mostly online, but everything that we do online is affecting everything around us. I mean, even within things as important as elections, you know, I know, in the US, they've got one coming up this year. So, like, there's so many things tied to our privacy.

Aaron Welwood 07:08
And I'm trying to remember the quote that David had, and it's like this famous quote, of, you know, how privacy is intrinsically tied to human potential. And it's true, because you need to have.... people need to have privacy in order to, you know, process things, their thoughts out loud when they have conversations with people, if you can't do that, it really stunts the growth of an entire society in various different ways, which I'm sure again, some of the other guys on the panel could speak to that in probably a much more philosophical level than I can. But yeah, anyways, I do think people care about it, it's just a matter of how much do they understand the issues that are tied to privacy, and that is going to become more and more evident, as you know, things like AI start to expand, it's gonna get pretty serious. And I think people will start to realise it in the next, you know, couple of years.

Darren Moore 08:13
Yeah, I was listening to podcast this morning. And they're talking about... it was like a Jordan Peterson podcast, and they're talking about the truckers. And they're like saying, you know, everyone wished that they.... everyone said that they'd be the person like hiding... But, you know, in reality, you don't know what you're capable of when the masses get like a hold of hysteria. So, you know, I really appreciate you guys are willing to work on privacy and push it to the limits and know that there is there's a lot of people that are against privacy for numerous reasons. Right. What do you think is the biggest enemy of privacy?

Aaron Welwood 09:00
Oh, my gosh, that's a big question. Yeah, I don't know. I guess I don't want to be provocative, but in my opinion, I would say the governments or just in general. I know, that's kind of like a sweeping statement. But that's just what comes to mind. And I don't mean that they're a threat to it intentionally, but there are interests, right. And governments have interests, people within it. Right. And I think that even unintentionally, our privacy, and essentially, our freedoms get threatened because there's this balancing of interests.

Aaron Welwood 09:42
And unfortunately, when the world is in chaos, you know, countries are in chaos. People want security. And, unfortunately, privacy seems to take a pretty big hit when people are demanding security Because of fear, and there are certainly players, you know, historically, (and we don't need to get into it, but I think anybody here probably understands it.) When there is a threat to our security, there are there are people that will try to take advantage of that. And that's unfortunate, but that's just the world we live in. So yeah, I guess that would be my answer. I think that governments, you know, intentionally or unintentionally are an ongoing threat to privacy and a threat essentially, to themselves as individuals, people that are in it. So, yeah.

Darren Moore 10:36
All right. So here's the last question, Aaron - what steps are we going to have to take to ensure that our children live in a world where they can have privacy?

Aaron Welwood 10:47
Wow. Yeah, adopt XX Network technology. If I can do a shameless plug! I think, you know, in the context of the XX Network, we're doing what we can, which is to make sure that important players in the market are adopting the technology that's going to protect humans, real humans. And I mean, really, that's all we can do. When you look at a big question like that, it seems very daunting, the average individual including myself, you feel like you can't do anything - you're like, who am I? Like, how in the world am I going to influence global powers. While I'll tell you how you, you join a community, you join a global movement of people and you work together, if you look at something like an individual, you're not going to likely be able to do much. But when you join together with people of like mine, you can make a difference.

Aaron Welwood 11:53
So it's as simple as if you don't know what else to do, you just start talking to people about it. And that's the importance of, you know, in the states that's like, first amendment rights or free speech, it's like, you need to be able to speak freely, even if you don't know what you're talking about, because that's how you grow. And start talking about privacy, start talking about the issues surrounding this, do your own research. And, and once you do that, get into groups where, where people are already doing something, that's, I guess that's what I would suggest to other people.

Aaron Welwood 12:29
That's what I've done. I mean, right back to 2017. You know, the guys that know me, and we're, you know, back then even Paul, like I mentioned, that got me into XX Network, we were looking into privacy communication online is something that where we felt like we were actually going to be able to have a conversation and not have somebody looking over our shoulder. That was it. So you just got to start somewhere and start moving. I don't know the exact steps, but just start and it'll work itself out.

Darren Moore 13:02
I appreciate the answers. Aaron, is there anything that we we didn't get to that you'd like to talk about? Or you think we touched on everything?

Aaron Welwood 13:13
No I think that's great. Thanks, Darren, I'm looking forward to hearing what the other guys have to say. I mean, we got... these guys that are going to be speaking and, you know, pump their tires a bit. People, you need to listen to these guys. They are, in my opinion, and I think if you look into their pedigree, so to speak, these are some of the top people in the world, in software engineering, cryptography, so on and so forth. You know, they have all worked under David Chaum. Some of them that's how they started their their careers. These guys are legit. And you know, David would say the same thing. So listen to these guys. They know what they're talking about. And I'm excited to hear what they have to say today. So thanks, Darren.

Darren Moore 14:00
Most people don't realise that like the big brain guys - they just come up with ideas. And it's up to up to people like Mario and Bernie to actually implement the ideas. They're not doing the coding, they're not

doing the groundwork. So with that being said, Mario, can you please introduce yourself and kind of what you do at the XX Foundation, XX Network?

Mário Yaksetig 14:26
Absolutely. Yeah. I hope my sound is working. I see the little icon moving so I'll take that... perfect. My name is Mario, cryptographer by trade. I was one of the first hires at XX. Rick was one of the founding members and you will know I was one of the first hires so I literally graduated straight out of college, David Chaum emailed me and he says I want to have a video call with you. Now keep in mind, this is a guy who I studied hardcore in cryptography classes in college right? So I was like, Oh, I'm like scared. I get into a call with him.

Mário Yaksetig 15:03
And he basically hires me and it was like the craziest story ever, because he calls me. This is like a Wednesday. And he goes, Yeah, so if you can move to LA this Saturday, we'll be very happy to have you. We'll take care of everything. And I'm like, what? Like David Chaum, the godfather of cryptography is about to hire me. I've always wanted to move to LA. I'm in Cayman Islands now. And it was it was mind blowing. So now yeah, so I'm more on the cryptography side, I like to consider myself an applied cryptographer. So actually bringing things into the real world. Rather than just writing papers and putting them on a bookshelf and trying to chase citations, I like to see technology in the hands of people.

Darren Moore 15:49
So you move to LA move to LA the second you got a job with David, where were you living prior to that?

Mário Yaksetig 15:56
Basically yeah. So I'm originally from Portugal. And I moved to LA right after - I just had to do some visa paperwork obviously. But that was it. Yeah.

Darren Moore 16:07
Wow that's quite the commitment. So can you share about what you've been working on at the XX Network?

Mário Yaksetig 16:17
Since we started, I'll give like... I know, time is of the essence so I'll try to be concise here.... So we started with a mix network, right? Having a private anonymous communication layer. And that has to be strong and fast, has to be very secure and fast. So that was the starting point of everything. It was number one implementing that. And Rick at the time was a massive, massive engine of this this whole development effort. It was building the mix network, and then that's kind of like the baseline, what do we need next? So now we need to kind of like rotate keys, we need to make sure that if a hacker steals Aaron's key, we need to rotate keys and that we can keep the conversations private.

Mário Yaksetig 16:59
So that was it. And then the more I kept working with David, there's something very important to mention here. Keep in mind that David has been warning about most of the issues that are happening now since the 80s. Right? So XX Network is basically what David believes should be a pedigree cryptocurrency and ecosystem... more than that... he always used to call it... he started when he was first like mentioning XX Network, he would always call it 'WeChat on chain', and people made fun of

him at the time. And now look at the narrative. Everyone goes 'the super dApp, the super dApp engine', like it's insane how wild he's like overlooked in these things. And so basically, the XX Network, I've been assisting David in all of these verticals, voting, governance, fast consensus, quantum security, key rotation, now we're doing very fun things with Worldcoin, the Worldcoin foundation, but I think I'll leave that for the upcoming questions.

Darren Moore 18:00
Yeah, so can you explain I've saw that XX was in the headlines with Worldcoin? Can you explain what's going on with XX and Worldcoin?

Mário Yaksetig 18:09
Absolutely, yeah. So a couple of months ago, Worldcoin foundation opened the wave zero of their grants programme. And funnily enough, a lot of the stuff that David and I were doing before, was very relevant for Worldcoin. And we actually used that always as a use case, we're like, oh, Worldcoin could do this, Worldcoin could do that. This would be better for privacy for the iris scanning, this will be better for the database. And so then I called David, and I was telling him like, David, you should apply for a Worldcoin grant. Because they will listen to you, right? Like, David is that cryptography icon like, they will listen to you. And this is what they need. And yeah, they didn't really know that we actually presented three grant proposals to them, and they accepted all three.

Mário Yaksetig 18:56
Basically, one is to add an anonymous communication layer to the scanning of the orbs. Right, unfortunately, but also fortunately, Worldcoin foundation was under a lot of heat. For privacy reasons, it's not really ideal for a single entity to have all those IrisCodes in a database. And God knows what they can do with that, right. And but they are very privacy conscious. So keep that in mind. And that's why they supported our three applications. And so one was to add the cMixx what we call cMixx, the engine of the XX Network, to overlay to hide the origin of those orb uploads and to add an additional privacy layer. That's number one.

Mário Yaksetig 19:39
Number two is a coercion resistant voting scheme. So it's basically a very secure and easy way of voting from your phone. Even if you are being coerced. Like there can be literally a guy with a gun pointed to your head, he steals your keys. He votes for you, and then you can still vote the way you want - it's very strong. As far as I know, it's the strongest voting scheme I've ever seen. Which is very important for crypto governance, right. So keep in mind that a lot, a lot of the way blockchain voting is happening right now is effectively pretty weak. And we are trying to change the game.

Mário Yaksetig 20:19
And then number three is what is called in the community cMixx+. So it's like an extension to that engine that we have - cMixx. Informally, on the outside, we also call it Zanzibar, like David and I found the name catchy. So we just go with that. And that is basically a way to allow Worldcoin to have the same database with all the IrisCodes, but fully encrypted with lightweight cryptography so that it's fast. And then people can scan their eye, encrypt that payload, and they can check if that entry is there in the database or not. Which is very powerful. Right now you can kind of authenticate people without really knowing who is authenticating. Those are the three verticals. And I'm happy to build on any of those rabbit holes.

Darren Moore 21:07
Yeah, I mean, it sounds really interesting with everything that's..... I mean, like Worldcoin went through through a lot of flack by the crypto community by scanning everyone's eyes, right. I believe me and Rick are actually talking about this. On one of our streams, we're actually talking about like the implications of what that would mean. So how are you protecting everyone's privacy in a protocol where people's eyes are getting scanned, like that and being stored?

Mário Yaksetig 21:40
So basically, what we have, it's something pretty interesting, it dates back, it's like a variant of the mix network. The best way to put it is like a perpetual mix network, where the whole database is a sequence of encrypted IrisCodes. So you have no idea who they are, like, which IrisCode, is which. And then every time a new IrisCode is added, it gets encrypted. And then say that the time is very flexible. But imagine every five minutes, the whole list gets reshuffled. Now you have no idea, maybe you knew that a specific encrypted IrisCode registered now at 12:24.

Mário Yaksetig 22:16
But five minutes from now you have no idea which of the IrisCodes is that one in the in the database anymore. So that's the rationale there. Here, the beauty of that approach is that you don't really need very fast like, very, very low latency, it can take a while, because you're just periodically re-encrypting the database. So it's not like you have to do it every millisecond. You know what I'm saying? You can only do it that like every five minutes every hour, then it depends also on the type of security and privacy you want. But it's very flexible. The cryptography it's very lightweight. So it's an ELGamal re-encryption, that is very well studied. It's pretty straightforward. That part of the of the system.

Darren Moore 23:01
So cMixx+ that's running on on its own cMixx, or is it tapping into the old cMixx? Or is it it's a separate version of cMixx?

Mário Yaksetig 23:12
So it's a separate version of the mix network. And it gets us a very interesting, kind of like caveat, in the sense that now we have somewhat of an autonomous system. But that is also based on the original premise of the whole XX Network. So what we are trying to do now is we opened to the node community to help us run and decentralise this, this mix network, the cMixx+.

Darren Moore 23:41
So I'm wondering if I am I allowed to ask you about anything that's going on with Project Tourbillion?

Mário Yaksetig 23:49
You can absolutely yeah. Now now that the books are open, you can.

Darren Moore 23:54
Alright so what did what did the BIS learn from Project Tourbillon?

Mário Yaksetig 24:00
So a couple of months ago, just for context, David Chaum and I were technical advisors to the Bank for International Settlements. So it's one of the biggest banks in the world. People call it the 'Central bank of Central banks', right. And we were advising them on retail CBDC that provides cash-like anonymity.

So this is it's very strong. I can even say this again. It's literally a CBDC for the public. That is private. Right? So this completely killed many rumours that existed that like CBDCs were just for a big brother surveillance system. We actually tested that out with.... even some data from payments in Switzerland from a couple years ago so that we could model its performance.

Mário Yaksetig 24:51
The main lessons learned were that the project itself was trying to explore three things. It was privacy, scalability and security. And by security, they wanted to explore quantum security. Alright, so this is a lot to test at once, right? But they wanted to go big or go home. So that's what we did - the lessons learned were, there's a lot of caveats, right, with every single decision comes a trade off. So if you win something in privacy, you're probably going to lose a bit in scalability. If you win something in security, you're probably going to lose.... that type of stuff, right? The lesson learned is that it's very viable and possible using the existing technologies (and Tourbillon happened to be fully powered by cMixx, our mix network), to other privacy oriented CBDCs for retail, which is very good, right? So don't let anyone fool you into 'Oh, you cannot really have privacy!'. You can. If anyone is trying to tell you otherwise, they're probably lying.

Darren Moore 25:55
Yes. So this is important because if anyone says anything about a central bank, digital currency, not being able to have privacy, now they have all the proof in the world, they could just show Project Tourbillon there was privacy with this, you see? So it is possible to have it. And... that's great. I mean, most people are fear mongering CBDCs. But with Project Tourbillon, you could, you know, pretty much prove that there's privacy available for people that they want it.

Mário Yaksetig 26:29
Yeah and rightfully so like, it's very valid for people to be afraid of what can come from that - it's a very valid concern. And David really wanted to prove... that was David motivation all the time - it was literally, I want to prove to the world that if anyone tries to tell you that you cannot have privacy in the CBDC, that this would work. And we happen to end up with working with one of the biggest banks. So it was case closed, almost.

Aaron Welwood 26:55
Can I just add just one thing there Darren? So just on that, what David did - it, it kind of went both ways. Not only did it prove it to the public, it proved it to the banks. It proved it to the other CBDCs that are being built, the other people that are doing these projects, say hey, don't say, oh, we can't do privacy, it's too hard. No, you can do privacy. And this is how you do it. So it not only proved it to the public, it proves it to the banks.

Aaron Welwood 27:30
So I just wanted to mention that because I think that was also important to David as well. Because he believes (I guess I shouldn't put words in his mouth), I think that he understands the threat of banks and governments that, again, may have good intentions, but they could inadvertently hurt privacy and then end up hurting democracy, if they mess with our money systems and remove the aspects of cash that we benefit from. So anyways, that's my opinion. I'm pretty sure that's kind of the spirit behind David is he's really trying to protect people around the world, and sometimes from themselves. So that's kind of what I mean by that, anyways.

Darren Moore 28:23
Well, well said Aaron and I think you hit the nail on the head, I mean, just being able to prove to banks and central banks and governments that it is possible to have these technologies and keep them private at the same time, that should be the focal point. So, Rick, I know you've been working on quite a few things. Can we just talk about some of the things that you've been working on. First, can you introduce yourself and your background with the XX Network?

Rick Carback 28:52
Yeah, thanks Darren. I've been working with David since 2005, when I met him after he gave a presentation at my school. And so we're coming up on the 20 year anniversary. So I guess that qualifies me as kind of an OG in the crypto space. I've been doing miscellaneous blockchain adjacent projects, voting projects. We got back into this, you know, after the initial cMix paper, and the last five years or so I've been working on this project, more or less full time.

Darren Moore 29:33
So you've been working on a library for the xxSDK. Is that Is that correct?

Rick Carback 29:41
Yeah so the current focus right now is to make it a little bit easier for people to use the XX Network inside of their project. And what we've decided to do is make libraries available for iOS via CocoaPods for Android via a Maven package, and for the web via an NPM package. So if you're a developer, you know what all those mean. But the general idea is you can type a command or set a configuration, and you've got XX Network libraries in your application. And then we're going to be documenting.... Okay, once you've done that step, how do you actually work this thing in to whatever it is you're trying to do in your application?

Darren Moore 30:32
So for people that doesn't understand what that means is that he's created little commands that if you're a developer, you just pull the command and drag and drop it into your whatever you're building and it's easier to code that way than to learn to code everything by scratch. And this is customised for the xxDK. So you mentioned that it was specifically for WASM WebAssembly, is that true?

Rick Carback 31:04
Yeah. So the the the JavaScript package has what's known as WebAssembly, which is essentially binary applications that run inside of your web browser.

Darren Moore 31:19
So I googled, like some sites that used WASM, like, what are some examples of it, and it had, like AutoCAD, Google Earth, different sites like that. So those are, those are WASM sites?

Rick Carback 31:34
Yeah so anything that is very difficult to get working online - I would guess that Microsoft Office, the Office Suite is using a lot of WASM. And what they're doing is they're taking traditional desktop applications. And they're compiling a large part of it, essentially, all the stuff that does the work, into a binary that's fit for your web browser. And then they're building a UI that accesses that binary. Because we have a lot of sophisticated encryption, we've got post-quantum libraries, we've got end-to-end messaging libraries, we've got the API into the cMixx, servers, all of that stuff is built into that

WebAssembly. Binary. And that enables the developer to access it like they're, they're running it on a desktop computer.

Darren Moore 32:23
Yeah, so I can imagine privacy being like paramount in those situations, right? So if I'm running a virtual type of application through a browser, right now, I need my credentials to log into that. If it's Google Earth, right, like, it's telling me my, where I'm located and everything. So I can imagine there would be quite a bit of utility for for developers to create privacy apps that tap into both WASM and the xxDK. What was one of the examples that you are thinking of when you're building this library?

Rick Carback 33:04
So our vision... I'll just, I'm sorry, to change the nature of your question... But I think our vision is to make this as easy as possible for developers to integrate. And in the context of the web, to me, that would mean... it's known as a React component - if anyone has ever looked at HTML, it's like an HTML tag. And you can include an HTML tag in your website. And it defines who you're going to communicate with, and then you deploy that to your web server, and then you'll have a little box that can pop up. And then anybody who goes to that website can then talk to that person that you set up to be able to talk to.

Rick Carback 33:50
And you can be running, you know, an app on your end, that you receive these messages and respond, right. So I would love to see something very simple, where even a, you know, not a programmer, but someone relatively tech savvy, can say, oh, I want to add a chatbot to, you know, an xxDK powered chat bot, where I'll get the messages or I'll hook it up to some AI. But it'll preserve the privacy between the two communicating parties there. And I want to see those kinds of widgets become available on the system when we're doing this.

Darren Moore 34:27
So make it as easy as possible for developers to integrate it into whatever they're building. And that's, that's the importance of having the libraries, is to make it as easy as possible. So that's correct, right?

Rick Carback 34:41
Yeah and there's always going to be depending on the context, customization needed. If you're building a desktop application, it's very different from building a web application where a widget makes sense, right? You might want a simplified library where you have better control over how the AI looks, how the UI looks on a desktop app versus the web. And, you know, we were trying to get it so that there's an interoperability between all of these components. So if you're building for desktop and the web, there's essentially no work that you have to do to make sure that they can talk to each other over XX Network as well.

Darren Moore 35:28
So the whole idea behind this cMixx is you're going to need to pay postage with XX tokens that like goes through cMixx, you pay the postage, and that's how you get privacy. And what Rick is doing right now is setting up libraries to make it easier for developers to integrate any type of privacy into their application, he focused on WASM. So that's, so that's like virtual machines on the on the web. So applications that are on the web, I can imagine a tonne of different reasons why you would want privacy, just crypto exchanges in general, right?

Darren Moore 36:07
If you're having having an xxDK on a crypto exchange, and you're able to keep people's privacy that way, that would open the door for a lot of different things. And then, you know, everything in the background using cMixx. And then, you know, that's that's where the utility comes in. So I can see a lot of different use cases for all this. So you mentioned NPM, as a library, what type of commands help developers if you have a library already suited for xxDK and WASM? I'm assuming devs save a boatload of time with with the NPM library?

Rick Carback 36:49
Yeah, so NPM stands for Node Package Manager. Node is a JavaScript technology for running web servers. And it is also relevant for deploying websites as well. And in the case of an NPM, someone who's working in that ecosystem, all they have to do is "NPM -install xxdk -wasm". And that command will work right now. So if you're sitting at a terminal, you can actually type that and you'll get our package installed.

Darren Moore 37:25
And and so you install this and you can start tapping into cMixx today?

Rick Carback 37:31
Right then you're coding in JavaScript, you import xxDK WASM. There's a little bit more to it. But yeah, in about 50 to 100 lines of code, you're in business. So the the barrier to entry is pretty low for a developer right now, you still have to read some documentation, but it is quite accessible at the moment.

Darren Moore 37:52
Awesome. So right now developers can pretty much tap into one of the best Privacy softwares out there and it's just understanding that they need to type this code to enter the library, and then start accessing commands. And that can protect a lot of the things that they're doing, whatever they're doing, and they get to protect whatever they're writing.

Rick Carback 38:20
Yeah and our goal is, at the end of the month, to have all of this well documented with simple examples. So you'll just be able to copy and paste it into your code, and it'll be working.

Darren Moore 38:30
So that sounds that sounds like a huge, huge feat, except for it's difficult to understand. But it sounds like you know, once everything is up and running, a lot of people will be using this because it bypasses a lot of... if I have to code this myself, who wants to rewrite the book, right? If I if somebody else coded for me, I just drag and drop it in. And I don't have to write the privacy, I just just piggyback off of what Rick has already built for me. And that's kind of the whole idea is just copying and pasting what Rick has built. Is that right Rick?

Rick Carback 39:11
Yeah. And I'm looking forward to the feedback loop that hopefully comes out of that, in terms of "this doesn't make sense to me", or "can you make this simpler?" That's definitely a goal. And we've seen it with other people who have integrated their private projects into the XX Network. Certain concepts are

kind of foreign to them. So how do we explain that to people? How do we communicate why this matters?

Rick Carback 39:39
One of the big things that always trips people up is that there's a transmission ID versus many reception IDs. So the reception IDs... there's a route, and then there's like a key derivation on the reception ID so there's essentially infinitely many, but on the transmission side, there tends to be one because you are eventually going to need to pay for postage and you're gonna have to fund that account. And that transmission ID is never associated with the reception IDs. In fact, the reception IDs are somewhat throwaway, because you've create new ones all the time, depending on which library you're using. So it's very easy. I could go nerd out on this for days. So I'll cut myself off, there

Darren Moore 40:18
You're saying the thing you're most excited about is people actually complaining about the thing that you built. So you can help walk them through it, after they complain - that's what you're looking forward to?

Rick Carback 40:32
I would not say it that way, I would say having users and getting feedback. But yes, more or less.

Darren Moore 40:39
Yeah, I would take it as people complaining about it. But I mean, at least it's getting used, right. Like that's the whole purpose is everything's getting used.

Rick Carback 40:51
We've been working with professional developers who I would say, are as smart or smarter than we are. You know, they're working at banks, or they're working for some unknown entity. That is, they're not communicating that to me, right? And they're saying, "Oh, we need this post quantum algorithm." And I'm saying, "Oh, yeah, you can use this", like very complicated thing like, "Oh, yeah, I finished that, it's on this branch." And then I never hear from them again. But if we want this in the hands of the common man, we need to get this into the hands of the common developer. And this is sort of a first step.

Darren Moore 41:29
Right, and then writing all the documentation that goes along with that, well, the common developers asking you all these questions, you're documenting all that, and then it gets put out to the public. So everybody gets it.

Rick Carback 41:43
Exactly. Everybody benefits.

Darren Moore 41:46
Well, I'm really looking forward to seeing all this come to fruition. I know you guys have been really cranking on it, and spending a lot of time working on everything - it's gotta be a killer, to spend all the time coding everything. And then starting to see things actually develop and build over time. So I wanted to get to Echoexx. And that's something that Bernie and Baltasar are working on. So Bernie, can you introduce yourself and what your background is at xx?

Bernie Cardoso 42:25
Yes, my name is Bernie. And I've been with XX Network since almost the beginning as well. So after Mario joined, I went to university with Mario. So we're longtime friends. And yeah, it's been an exciting journey. So as part of the initial team, I started working on cMixx as well with Rick and Ben. And then when we started to launch the blockchain, I was part of the team that was in the Cayman Islands and researching new consensus algorithms for quantum security and actually launching the XX Network blockchain that supports the mix network.

Bernie Cardoso 43:01
So yeah, it's it's been an exciting four or five years now. And yeah, now, I work with Baltasar, and Mario, we have our development company called BitFasioned and yup, we are coming out with our new product called Echoexx, which again, it's building on top of all that has been talked before by Rick. So now that the xxDK is a bit more available to the common developer, like Rick said, we can easily just start building apps with it.

Bernie Cardoso 43:33
And that's exactly what we did. So with Echoexx, it's a new type of messaging app on the XX Network, which is slightly different from the ones that came before it, if you know the history. The idea for Echoexx is to be more crypto native. So you have a wallet, you log in, you can message anyone else that is on the app, just by their wallet or by by their ENS name. You can send payments in the chat now. That's that's the main idea. And we have a very exciting roadmap and features that we want to implement. But yeah, that's very, like a quick introduction.

Darren Moore 44:12
So Echoexx, this is running on different blockchains right now, right? This is kind of talking to wallets - so a wallet could talk to another wallet, per se? What blockchains is it currently running on right now?

Bernie Cardoso 44:29
So we initially are targeting Ethereum so you can log in with any wallet. We've tested mostly Metamask - I've tested other wallets as well with WalletConnect and all that. So you can just log in with your wallet and you can start messaging other wallets that are in the app as well. So those messages are fully private, they run on the XX Network. That's the idea.

Darren Moore 44:57
So only I and the receiver can see the message, right? So if I sent you, from my account, it would only be me and you that see the message that I wrote. So let's say you're holding my favourite NFT. And I wanted to buy that NFT from you. I could say "Listen, I want to buy an NFT from you, but I don't want to make my offer public, but I'll give you 20 ETH". Right, so it would just be me and you that would see the messages?

Bernie Cardoso 45:25
Yeah, we're starting off with the ENS chats, right? So one-to-one, private chats. We have ideas to create group chats in the future as well. And also to support the other networks. Of course, we're starting off with Ethereum, but we eventually want to expand to other networks as well, the idea would be that - the end goal would be that, no matter which ecosystem you're part of already, you can just log in with the wallet you use most commonly and just chat with anyone else basically. And I think that's a really powerful goal.

Bernie Cardoso 46:05
And... most people are probably familiar with Farcaster now and Warcast. That's been making the rounds a lot lately. So what we've built, it's quite similar. So Farcaster is a protocol layer. So anyone can implement a social networking app on Farcaster. But Warcast is an actual app that's developed by the developers or Farcaster as well. But it's closed-source, and you can pay to use it. And if it goes down, it goes down, it's happened, like they have bugs, they have to fix them, they have to deploy fix or whatever. All of that doesn't matter, because the base layer Farcaster is still operational, right. And this is quite parallel to what's happening with XX Network.

Bernie Cardoso 46:55
So XX Network, and cMixx is the base layer, it's the protocol layer. It's been running very smoothly for almost three years now - if you count betanet, four and a half, five years. And the main difference is that at that base layer, it's completely privacy protected. So there is no way to track the messages between senders and receivers. And that's something that none of these other base layers, protocols like Farcaster, Nostr, XMTP, whatever other things people are using nowadays, for web3 messaging (which there are some out there already), none of them respect the user privacy.

Bernie Cardoso 47:34
So, they are end-to-end encrypted, of course, but none of them are respecting user privacy. All these nodes are sending - gossiping, we call it - messages to each other. Like I want to send a message to you, it has to go through some notes. They can all see my IP address, they know where it's going, that it's going to you. This is all plain and simple to see for these node operators. The real powerful thing about XX Network is at the base layer, at the protocol level, none of this exists all the metadata is shredded.

Darren Moore 48:06
So to explain that to people that don't get it. So if I'm using Nostr right now (it's supposed to be running off of Bitcoin) and I'm tapping into bitcoin's ultimate decentralisation - their nodes are spying on me. Is that correct? Like they could be spying on me, taking my IP address and selling that information to somebody?

Bernie Cardoso 48:30
Yes, they're trying to tap into Bitcoin I think in some other ecosystem, it's not really related to Bitcoin. It's just a protocol, right? And the protocol that just says "Okay, we want to be a decentralised social network." Okay, cool. That's all great. But when you run a Nostr app, like you want to run the app and see, okay, I'm gonna message someone or are gonna receive a message, you have to connect to a relay node, I think that's what they call it. I think Rick knows a bit more about this, but it's either called Relay node or something like that.

Bernie Cardoso 49:01
So that relay node, it can see your IP address, you send it a message, it knows, oh, Bernie sending a message, he's sending a message to there. And here's his IP address, and then went there and goes to that same relay node, he knows, Darren has this IP address. That's it, like, you know, exactly who these people are, where they are. And, you know their metadata, when they send the messages, how frequently they talk.

Bernie Cardoso 49:25
All of this, in XX Network already doesn't exist, because when I'm sending a message over cMixx, the metadata is shredded. So when you talk to a cMixx gateway, or cMixx node, they know that you're sending a message, but when the message comes out the other end, and the nodes don't know anymore, where it's going or where it came from - sorry, they know where it's going, they don't know where it came from, so they don't know your IP address. So all your metadata has been shredded. And that's the really powerful thing of having XX Network as a base layer for any social networking protocols that you can build on top of.

Darren Moore 50:06
Yeah, so having having all the data shredded from the get go, that's the real thing with having any of the social media apps because I mean, a lot of them are claiming that it's decentralised and all this great stuff's happening with it. But if any of them gained adoption, the same exact problems could happen, right? Like, the only reason why it's not happening is because it hasn't been adopted yet. But if it was adopted, if Nostr was adopted like Facebook was adopted right, then then all these problems would surface and bubble to the surface, and then you would have to find a solution to all the problems. So that's pretty interesting. And I haven't thought about that.

Ryan Solomon 50:53
Hey, Darren, just to give you guys a heads up, I pinned up to the top - the first pin tweet, because I know that you guys just launched the new Twitter for Echoexx. So I think we have over 100 people in here, a lot of people will be listening to this today. This tweet: "Welcome to a new era of privacy. Echoexx is where your messages stay yours period - think of it like sending a letter that only the right person can open. No peaks, no leaks." But I pinned that up to the top. So for all the audience down here, go give Echoexx_tech a follow there. They just launched this. So there's less than 100 followers right now. But if you care about privacy, and you want to leverage tools that can actually keep your messages and keep your data private. Echoexx - give these guys a follow real quick. Sorry to interject there.

Darren Moore 51:42
No, not at all. I appreciate you saying that. Also, it's app.echoexx.tech - you could demo this right now if you want to. And you can write messages to people's wallets and everything. So that's pretty cool. So is there anything that I didn't get to that you guys wanted to talk about that I didn't get to?

Mário Yaksetig 52:10
Darren I have a story that I promised the XX community, super quickly! So basically, I used to travel and I still do a lot with David. So either for fundraising, for conferences, or whatever. So and as you can imagine, David is very popular. So he gets a lot of interviews by journalists. So at the end of interviews, David gives his phone number so that people can talk over WhatsApp, Telegram, whatever it is, and the sharpest one realised that David's phone number is an equation. And so David says number (unfortunately, I cannot leave many hints here, otherwise, I'll be giving the phone number away!) But he basically gives a phone number away and then people always respond - the sharpest ones. And they go "Wait, like the power of these numbers..." And he goes "Yes, I had to fight very hard for that for that number." So it was just a fun fact, just to show how mathematician he is.

Darren Moore 53:04
So giving people the wrong phone number but it was really an equation to the right phone number of people have to figure it out just to get in touch with David?

Mário Yaksetig 53:14
No the pattern, the pattern of the number itself if you follow it - the way the numbers grow, they are powers of specific number. Yeah, that's it.

Rick Carback 53:30
I have a closing thought, which is that Mario and Bernie and Baltasar all give me too much credit. You know, Echoexx did not rely on the NPM package. They built that out on their own. It's, you know, an excellent product from what I've seen, Mario's contributions have been amazing. So I just want to point that out. These guys are all top notch in my book.

Darren Moore 53:57
I had a chance to test it out. And it worked very smoothly, it's writing with Aaron's wallet. And we're going back and forth chatting with each other through our wallets. So I think it's a good use case too. Because you know, I get messages sent to my wallet and it's usually spam but you can tag people's wallets that are that are bad guys. Right. And so you know, don't don't interact with this wallet. You can you do a lot of different stuff with it. So I think, you know, it's just the tip of the iceberg. And once people start thinking about different use cases, the use cases will start emerging.

Bernie Cardoso 54:40
Yep, I see the Hashpack is here as a listener. So I've always remembered one use case that we discussed a few months ago where I think someone in the Hedera ecosystem was doing an NFT gated chat thingy. And I loved that use case for Echoexx as well - just have a group chat, where to enter, you actually need to own an NFT on a specific collection and you could just chat about that collection. I love that.

Ryan Solomon 55:08
Yeah, I think we had that. I know... it's always interesting, because we talk to so many different ecosystems and projects, it's like, we always try to find synergy wherever possible, and at least to foster relationships, because maybe, you never know, especially as innovation continues, and these projects continue to grow and develop and the space really continues to mature - having those relationships in place - maybe it's not something to action, like, immediately, but it's like, "Okay, we talked about this X amount of time ago, and now it's a perfect opportunity to do x, y and z." So I'm always trying to make those types of things happen.

Ryan Solomon 55:43
I have to give a huge shout out to Darren, thank you so much for hosting this entire portion. I know you're gonna hang out with us up here today. Aaron from XX, it's always nice to hear your voice I'm off to catch up with you on the side at some point. Mario and Bernie and Rick, 100% it's great to talk to you guys and congrats on all the new initiatives and looking forward to continuing to see you guys grow and build out tools that protect individuals privacy across the web three landscape, so really appreciate it.