XX Network & Worldcoin Grant Projects Discussed in More Detail with Mário Yaksetig and Patcrypt.

Mon, Feb 19, 2024 6:10PM UTC

SPEAKERS

Patcrypt, Mário Yaksetig

Patcrypt 00:00
Hi, Mario!

Mário Yaksetig 00:01
Hey there, how are you?

Patcrypt 00:02
I'm good. Thanks. It's really good to hear from you. And I thought it would be a really good opportunity for us to talk about the Worldcoin grants that obviously are getting the community of the XX Network very talkative and excited. And I think I think there'll be people out there and myself included, who would really like to know more about each individual grant project and what it means for the xx network and what it means for Worldcoin, and how they integrate - how our technology in the XX Network will benefit them, and how that same technology can be used for us down the line as well. So before we get going on the grant stuff, I'm just wondering if you could give us a little bit of an introduction about who you are and how long you've worked for the XX Network? And I think last year, you started BitFashioned and what that company does, and, and yeah, if you don't mind.

Mário Yaksetig 01:05
Absolutely, thank you so much for having me. It's very exciting to talk about these things. I think it's actually the first time we're publicly discussing what the grants actually entail. So this is a very exciting interview. So my name is Mario, a cryptographer by trade. My first job was actually straight out of college with David. So I'm originally from Portugal. I did my master's thesis in Baltimore. And then David read my master thesis. And he hires me right after that, which is very nice. I'll say that it! It was also a bit scary, because like, I had studied stuff that David created, and literally my first interaction with David was in him trying to hire me. Definitely very unexpected.

Patcrypt 01:49
I can imagine that's a bit of a 'star-strucking' moment!

Mário Yaksetig 01:51
Yeah, absolutely. Yeah, exactly. And so that was my first job, I believe that dates back to 2018. So I was one of the first hires at XX Network. And I've been working with David since, right. So David and I get along very, very well, we talk a lot, we create a lot of nice protocols, which is, we actually have created a lot more things. But we cannot just dump everything into the community because we go through like a somewhat formal process where we write up some security analysis, do some performance evaluations. And David also has kind of like this amazing, terrible trait at the same time, where he always improves the protocols, as the weeks go by. So some projects end up being in an always improving state, which is amazing. But sometimes, I know the community wants more and more. And we have a couple of things on the on the shelves right now. Presently, I founded BitFashioned along with some people that we were supporting here, the Cayman headquarters and BitFashioned is basically the main contributor to the XX Foundation right now. So all of the things you're seeing out there, Echoexx, all of the grants, that is still the core team, the core team that was in the Cayman headquarters, basically just rolled over to BitFashioned and completely supports the xx Foundation.

Patcrypt 03:21
And it makes a lot of sense to have that separation as well. Because you can work on related things or in other projects that can benefit our network down the line without feeling too, you know, obligated to be purely on our stuff constantly.

Mário Yaksetig 03:39
I think that's the biggest advantage. Yeah, we're now able and you're seeing that now, due to the separation, we're able to integrate way more things with way more people as opposed to before it was kind of like a more strict compartmentalised role, versus now we wanted that separation and expansion at the same time.

Patcrypt 03:56
So can I ask when you first saw WorldCoin, like what was your first experience of reading about it or hearing about it?

Mário Yaksetig 04:08
My first experience was it dates back a while ago, a while a while ago, so it was when the project actually came public on Twitter. So I'm always seeing what's happening on Twitter. I'm not super active, like posting stuff, but I'm always there. So if you want to message me on Twitter, I'll see your message for sure.

Patcrypt 04:28
I often see you engage with other people who get things wrong. I really enjoy reading your threads actually.

Mário Yaksetig 04:34
I'm trying to I'm trying to now trying to be a bit more active now. A lot of people are pushing into that because I tried to be kind of like that little watching person. But a lot of people are like, "You should step up and actually correct people because there's a lot of misinformation out there. And you know what's happening."

Patcrypt 04:50
Yeah, well, I mean, it's just nice to be able to see somebody with authority who really understands you know, the the guts of this stuff, the cryptography itself. You know I'm somebody who you have to tell me that stuff like I'm five years old, to be honest. And you know, me and you have had a few conversations where I've been like, "Can you just say that again In more words?!" So umm, I think yeah...

Mário Yaksetig 05:15
So I saw Worldcoin on Twitter. And funnily enough, that reached David as well. So shortly after, like a day or two after that appeared online (so I found out about it on Twitter), David called me and David was like, have you seen this? Like, a lot of stuff that I've been creating and stuff that we've been doing internally would solve a lot of the complaints that people are triggering, because when Worldcoin started, they got a lot of backlash. They got a lot of backlash.

Patcrypt 05:47
That's why I asked because when I first saw it on Twitter, I, you know, my first reaction was, Oh, God, they're, you know, scanning people's eyeballs. Where's this going? It's terrible, dystopian, awful.

Mário Yaksetig 05:59
It's kind of like the big brother nightmare. And they're very well intentioned. Keep that in mind. But coming from an outside perspective, a lot of people just saw that. And they're like, "Yeah, we don't really want those scans on a database that you control", right. So they took it very personally, in a very good way. And they decided to open these community grants. And they actively, basically reached out to everyone and said, listen, if you guys want to help us out with a couple of things, so the grants that they have in Worldcoin, they have a couple different categories. So they have a request for proposals, the famous RFPs, they have some open ended tracks. And there's other other types of integrations.

Mário Yaksetig 06:41
We saw that this was a match made in heaven, right. So we actually applied for three grants. And I can go over that just like a high overview, and then dive deep into each one of them. The first one, and this is actually a fun story to share. Because I think only the Worldcoin guys know this. But the grants opened. And actually, the day they opened the Worldcoin Foundation, they had an event here in Cayman. So I live in the Cayman Islands. And they went to the event. It was a great event. They're super nice. They're very, very technical. They know their stuff. Like it's always very good to see people who know their stuff. And they announced in that event, like by the way, the grants just open.

Mário Yaksetig 07:27
The next day I go home, like the same day I go home. And the next day, I look at the website, like the grant application. And I see that they have a couple of interests, they have a couple of open RFPs they're very much aligned with the stuff that we're doing, right? So I submit right away grant proposal for VoteXX. And I'll go over what VoteXX is shortly. So we submitted a grant application for VoteXX, and literally the day after David called (David calls me almost every day, we talk a lot about cryptography things.) And David calls me and I told him, David the Worldcoin grants just opened and some of the stuff that we're working on - so what is known by the community as cMixx+, but known by me and David as Zanzibar, that was name I liked.

Mário Yaksetig 08:13
So David wants to propose that name. And I liked it. So we're going along with that. And I told him, David you should actually apply like we should apply with Zanzibar, because Zanzibar started from the project with BIS (the Bank for International Settlements), there were a couple of things we wanted to improve on. And the problem is very similar. And again, I'll dive deep into what Zanzibar entails. And so I told David, and he was like, "Yeah, I don't know."

Mário Yaksetig 08:43
And funnily enough, like the next day after I get an email from Worldcoin Foundation, saying, "We would like to talk with you more to see what VoteXX is all about." This sounds very fun. Right? So I talked to them. And they're big, big privacy aficionados, like they really like privacy. And during the call towards the end of the call. I told them I was like, "Listen, I told David Chaum to apply for a grant. I don't know if you guys think that makes sense!" But and they were like, are you serious? THE David Chaum. I feel like "Oh my God, tell him to apply for sure!"

Mário Yaksetig 09:16
I called David that afternoon. And I was like, David, you should apply. So then we have a couple of long calls. David is so perfectionist, like... one word in a sentence that he doesn't like it has to be like rewritten to be like, the lowest detail... lowest level detail - he's very perfectionist, which is very good. It's a trait I admire. And so we spent multiple days, multiple hour calls going over the grant application, what that would look like, what would be the scoping because it's not just trivial. Not just something you do in like a month and then that's done - it requires a lot of development. It requires a lot of scoping. It requires infrastructure. Infrastructure these days. can get out of costs too quickly. It's not rare for a lot of startups to have obscene AWS bills, and other cloud providers. So we were talking and then David applied.... They were very interested to host David in the grants programme. So we had a call, I went to that call as well. And they loved David, they some of them have even written articles that talk about David. So it was, it was a match made in heaven. It was hilarious.

Patcrypt 10:33
It does sound like it.

Mário Yaksetig 10:35
Yeah, 100%. And then, I think a week or two later, I was talking with Aaron. And I went to look at the RFPs on the Worldcoin Foundation website. And I see that one of the tracks that they have, is that they wanted a network anonymity layer. And I was like, Oh, my God, this is us.

Patcrypt 11:01
Yeah, that is cMixx, right.

Mário Yaksetig 11:03
I was like, this is us! This is cMixx! This is what David created! It doesn't get better than this. I remember, I felt bad that I was already in two grants and I was like "Aaron, apply! But like, make it more XX oriented, because I'm already on two grants. And I don't want you guys to suffer! Because I'm already involved in two grants. Right?"

Patcrypt 11:24
I did wonder, I was going to ask if you could speak for all three, because your name's there on two and XX is the third. So it makes more sense. Yeah.

Mário Yaksetig 11:35
So we just played it safe, and we kind of have a whole prepping(?). Obviously, there's people are way more technical than me on the software side. So that was not really an issue. So they then talk with the Worldcoin Foundation team. I wasn't really involved in those calls, as I just mentioned. But apparently, it went very well, because they got their grants. Right. Then those three grants were selected. Right. So I think now would be the great time to actually go deep into each of those.

Patcrypt 12:07
Yes, sure. Do you want to start with the one that you just talked about the one that's the generic XX Network? Do you think that's a good place to start?

Mário Yaksetig 12:15
Absolutely. So in the grants website, they were looking for this network anonymity layer. And what that would entail is, when you... a quick Worldcoin recap: So the claim to fame is that you scan your eye, and you are able to get like a key pair from your eye. And this would mitigate a lot of the problems that exists now with the uprising of AI.

Patcrypt 12:46
Yeah, because it'll be hard to prove that you're a human being when systems are all pretending that they're you instead.

Mário Yaksetig 12:53
Exactly. Even on the internet right now, with the latest developments of ChatGPT it's already very hard, and it's only going to get worse, right? So they took a very pragmatic approach, which makes a lot of sense. And a lot of people don't like it. But at the end of the day, it is a viable solution that does make sense, whether people like it or not, that's, more subjective.

Mário Yaksetig 13:15
But you scan your eye, and then from there, that Orb uploads your IrisCode to a database that they have, right? This is one of the problems that they recognise. And that upload comes from wherever the Orb is. So it's kind of like this here - so imagine if an Orb is in Portugal, in Lisbon, you would know that someone in Lisbon just scanned their eye and there was a new database upload, which is not great from a privacy perspective. It works very well, the system works very well. But it's not great, because you're leaking a lot of information about what's happened.

Mário Yaksetig 13:52
So what the general grant is, is a way to mask all of those communications. So a lot of the stuff that happens in the Worldcoin protocols would be routed over cMixx. So you would obfuscate where the messages are actually coming from. So instead of being like, Oh, someone in Lisbon just scan their eye, it would kind of be like, Oh, somewhere, one of the Orbs just scanned, which is way better improvement than the initial premise, right.

Patcrypt 14:25
And this would be code that's running in the Orb hardware itself.

Mário Yaksetig 14:29
So the Orb itself, talks to an API. So that API will instead of touching that API, it will touch ours first, and then it would, it would touch that API.

Patcrypt 14:42
Okay. So you would be running some some form of infrastructure to take it to the mix network?

Mário Yaksetig 14:47
Yeah, but a lot of that is already developed. So in the - what's called the xxDK. Right, so the XX Development Kit. A lot of that is already pre-built. Rick would be the best person to talk about that and I know he has a little easter egg coming up this week, he's going to try to make a new new release this week on that. But a lot of that work is already done - a lot of that infrastructure is pretty much ready. So it's an iteration that is not a heavy infrastructure running that we have to do.

Patcrypt 15:22
And there's a second part to this, where it's... are the users also interacting with... Is this the same project that the users would interact through the apps and use the mix network for that?

Mário Yaksetig 15:34
Yeah, so we're taking baby steps, but the goal would be to... every single communication that takes place would be routed over our mix network, that would be the ultimate goal and kind of like the pedigree solution for privacy for the whole system.

Patcrypt 15:49
And the great thing, is the whole thing is already... it exists, right? So, that's amazing. Yeah, so we're literally plugging it in.

Mário Yaksetig 16:00
Literally, yeah.

Patcrypt 16:01
Yup. Super. Sorry for keep interrupting!

Mário Yaksetig 16:06
No, no, that's it. I think that covers the general XX one. Just think basically, every single communication that takes place between the Orb to a database between apps between anything that they have, that would be routed over cMixx. Right now, Worldcoin has, I believe, 2.7 million users? Probably if not have already closing in on 3 million.

Patcrypt 16:32
3.4 I saw earlier today. Including me actually, I downloaded the app, but I'm not verified because there's no Orbs anywhere in the UK. Yeah. I don't know if I will, until it's full of cMixx stuff, either.

Mário Yaksetig 16:46
That makes sense.

Patcrypt 16:47
Yeah.

Mário Yaksetig 16:49
Anyway, but that's the that's grant number one, let's call it.

Patcrypt 16:54
Great. Okay, let's move on to Zanzibar.

Mário Yaksetig 16:56
I'll let you choose. All right. Yeah. Zanzibar it is. I was gonna say, Well, yeah. Let you choose.

Patcrypt 17:01
I've got them lined up in tabs, so I'm just going through them.

Mário Yaksetig 17:04
Zanzibar it is.

Patcrypt 17:06
Which was awarded the most amount as well. So does that imply that there's more development behind this?

Mário Yaksetig 17:11
Yes, yes, yes. There's substantial cryptography development that has to take place there. And there's substantial, there's a substantial infrastructure, substantial decisions that have to be made. That one is far from trivial. So that one is like a ground-up approach. The other one already has like the SDK, the APIs, is kind of like the stuff has already been pretty much tested.

Mário Yaksetig 17:35
This is kind of like - David and I wrote a couple of, I wouldn't call them papers, but documents describing this. And we've discussed this in multiple calls. And now we're going to fully implement the whole thing. And what this is, is - this ends up being very tricky to explain. But I think the easiest way to see this is literally imagine when you log on to whatever, Instagram, Facebook, Slack, or whatever you want to think of - that service provider, they have a database with all the users in the system, right? So there's a list of users and a list of kind of like hashed passwords traditionally, of people in the system. Now, this means that the service provider knows exactly what the users are and what the hashes of the passwords are. And it's traditionally centralised. It's a traditionally centralised database.

Patcrypt 18:37
Pretty much every website that yes, a login, yeah.

Mário Yaksetig 18:41
Anything that you can think of, and then you can... basically Spotify everything that you have opened on your computer is highly likely...

Patcrypt 18:49
Any service with users, yeah.

Mário Yaksetig 18:52
So, for that setting, that traditionally makes sense. Because you were a user, you want to log into Spotify, you want to listen to music, Spotify just allows you to actually access the resources. So that's kind of centralised, and they control all the information. But often, you want a database to be shared by multiple people. And traditionally, the easiest solution is, oh, let's publish the whole database on a blockchain instead of a single server database.

Mário Yaksetig 19:25
And that is fine if you're okay with actually revealing all of that information, right. But now, imagine this from the Worldcoin perspective. Do you actually want to put the IrisCodes of 3.4 million people on a blockchain for everyone to see? Probably not, right. It's not probably - hence why we got that grant. Now with Zanzibar, and this is something that started from the BIS project. So a couple of months ago, David and I were technical advisors to the Bank for International Settlements. It's one of the biggest banks in the world. And they were doing a private retail CBDC project inspired on work that David had done.

Mário Yaksetig 20:13
And one thing that we wanted to improve on was this notion of, there was, again, this database, it was all published on a chain, it was this notion of unspent coins. So the actual serial numbers of the coins that hadn't been spent yet, were all public. It was fine. It was fine. But David wanted more. Alright, so David was like, nah, it just doesn't feel right. I don't want to reveal any information there. So David, for literally, probably months, he has been working on this. And he really likes to use very strong primitives.

Mário Yaksetig 20:51
So for months, he was trying to come up with this kind of like, ongoing mixing of data. But you wanted to have it encrypted. So imagine you have this database, and all of a sudden you encrypt it. He's using ELGamal to encrypt it. All of a sudden, you encrypt all the data, so you no longer see what's on the database. You know how many entries there are, and some could be dummies. So if you also wanted to cover that, you could add some dummy entries, like you could encrypt zeros. And you wouldn't be able to tell which ones are real entries or not. And then you are constantly shuffling, or technically what's called a re-encryption mix - you're constantly re-encrypting that database. So now you no longer have a database where everything is public, you shifted that into a private database.

Mário Yaksetig 21:44
And you can constantly re-encrypt it and prove that you're re-encrypting correctly with very strong cryptographic primitives and very efficient as well, that's very important - the stuff is very efficient. And you don't even know. So if imagine I were to register on Worldcoin, I would literally go to the Orb. In an ideal world, that upload goes over cMixx, so they don't even know where the Orb is. In that exact upload, my IrisCode is encrypted, gets posted to the blockchain. At that moment, you just know that

someone registers and... a minute later, the whole database gets re-encrypted and shuffled. So you just lost track of the new person that registered in the system.

Mário Yaksetig 22:30
And if you want to make some lookups, then what you can do is the user is able to do some fancy cryptography and check without revealing the actual IrisCode, check if that IrisCode is whatever they're looking for, is actually on the database. So they're able to authenticate themselves without revealing the actual underlying data. So you would know where it collides. So imagine you're trying to log in on Spotify. I put my username Mario in Cayman. Spotify knows Oh, Mario in Cayman is logging in. In this case, they will just know "Oh, one of our users happens to be this encrypted person - is logging in", but they have no idea who that is.

Patcrypt 23:14
Okay. And where does the shuffling occur?

Mário Yaksetig 23:20
So that is one of the scoping things that we're trying to figure out. Ideally, we want to have everything on chain. So David, and I really like to assume a very strong adversarial model. But we basically want to give everything that is possible to the adversary. So we want to publish everything on the chain, we want to give control to as much stuff as possible. And then if we're secure in that setting, then we're golden, on a real world system.

Patcrypt 23:47
Makes a lot of sense. Yeah.

Mário Yaksetig 23:49
Yeah, exactly. So for now, the first version of Zanzibar will probably just be a simpler testnet, where we actually publish all the data, reshuffle it and then republish. But then, at some point, we're going big into like, actual main net and actually re-encrypt stuff. And that data could then be decentralised or Worldcoin could keep it in a distributed database that they own, but they would still have no clue of what's going on.

Patcrypt 24:21
Right. This reminds me of a conversation that we had a long time ago when you first published a paper about cMixx+, so is this what you would class as the plus?

Mário Yaksetig 24:35
Exactly? Yeah.

Patcrypt 24:36
Right. So is the ultimate aim for this to integrate fully into our main net of cMixx?

Mário Yaksetig 24:44
Yes, so obviously as a decentralised platform, we cannot really push this to every node. What's gonna happen is once it's fully coded, and if you remember a couple of months ago, I asked the node community if they would be open to running the binaries... is, this would be an add on. So imagine if

you are an node runner, and you want to participate even more. So if you already run cMixx, and you're okay with running cMixx+, which is going to be very light. So if you already have a node, you're more than golden to run cMixx+, then you could potentially earn extra revenue from that.

Patcrypt 25:22
Right. And is there a revenue model built into this? Is it just in conceptual terms at the moment? Because I'm trying to imagine what that could be? Is it just part of postage?

Mário Yaksetig 25:34
Yeah, there's a couple of ongoing discussions on that. I wouldn't say it's just purely theoretical, some of the things are pretty fleshed out. But as always, there's kind of like, a couple of different trade offs. So I'm not going to commit here to a single model, where we work has been done.

Patcrypt 25:52
Things change and things grow and things evolve. Fair enough. Well, that one sounds like a beast.

Mário Yaksetig 26:01
Yes. That one I'm excited for. I'm very excited for that.

Patcrypt 26:05
Great. And let's move on to the last one. And then I'll kind of round up what the three kind of mean in total and, perhaps, talk about what your priorities are and how you see it going. So let's talk about VoteXX. I actually read the VoteXX website, the other day, purely out of interest, and saw that it had been used a framework, if nothing else in a real world, mayoral election several years ago. Is that right?

Mário Yaksetig 26:39
So it was inspired, most of the team that was involved in that election is part of our team now. And some of the primitives used there rolled over to VoteXX. Okay. And with that, I think I can segue straight into what VoteXX actually is.

Patcrypt 26:57
Please do.

Mário Yaksetig 27:00
So, right now, everything is digital, right. So you send emails - people no longer really send letters, obviously, there's a couple of things that still go via the actual mail. But it's much less compared to 10-20 years ago. A lot of stuff is moving to the digital realm, right. And a lot of people want voting to become digital, because then that means you can vote without even leaving your house, right, which is, in a couple of elections, it's very practical, because sometimes you have to kind of like drive, it's a whole hassle to get to the place and you have to park then you have to wait in line, and then you vote, this can take a lot of time.

Mário Yaksetig 27:42
And abstention is traditionally a big problem in voting, like in regular elections. So in theory, digital voting would make things much better, because you could just vote from your phone or from your computer, and you're done. Now, it sounds very good in practice. But in reality, what that also means is that it's much easier to bribe people. Right? So it's much easier to literally go or even coerce, right? The

actual formal term in the literature is coercion resistance. But it's much easier to go to someone and be like, listen, here's 100 bucks, please vote for XYZ in this election, and you see the person vote in front of you. And that's it that's done. Or you can coerce right, a lot of people... and they estimate this, but you can easily imagine problematic families where, let's say, one person forces other family members to vote a specific way. That's a very realistic threat.

Mário Yaksetig 28:46
Or you can think of this, a bigger scale would be if a specific state in the United States doesn't vote for XYZ, then they're going to cut funding in a specific category of the city. So it's very problematic. And traditionally online, you are revealing who you're voting for. Right? So a couple of years ago, VoteXX has been going for a while. A couple of years ago, David (David has been working on voting and online voting for decades now)... a couple years ago, David reached out to me. And he proposed this idea of VoteXX. VoteXX - what it was then versus what it is now, it's actually fairly different.

Mário Yaksetig 29:40
The baseline remains the same, but a lot of the stuff became way better. So then we start gathering this team. David likes to call them The Avengers because there's a lot of powerhouses in the cryptography realm. And we were talking with them and they're like "wow, super interesting, count me in, count me in." And we, I remember we ended up being at some point 11 authors working in this and from pretty much a lot of different continents. We had people from the US, people from Canada, we had people from China. We had people from Europe. It was yeah, it was a lot, a lot of different a lot of different nationalities.

Patcrypt 30:19
A big problem that lots of people want to solve, I guess.

Mário Yaksetig 30:23
Exactly yeah, exactly. And this is also people that traditionally work in this space, and what VoteXX created is what I believe, the best coercion resistant voting scheme to date. And let's try to dissect what that means.

Patcrypt 30:42
So you're going to start talking about hedgehogs now?

Mário Yaksetig 30:46
Exactly. Yeah.

Mário Yaksetig 30:47
Right.

Patcrypt 30:49
I quite like that.

Mário Yaksetig 30:51
Yeah, that was, that's a pretty funny, that's also let's go, let's go down this rabbit hole very quickly. The actual term, if I recall correctly, that was created by David. Because apparently a hedgehog was used to stop tanks in the world wars. It was kind of like this little, you know, like, it's sort of like an x that you

put on the floor on the ground, and that the tank would be... they would destroy the tank's moving capacity. So David was very obsessed with the contrast of the hedgehog, the animal that looks very cute, versus the hedgehog tool used in World War that was massive, it was very simple and massive against tanks, like one of the most powerful things that you can use in a war, right?

Patcrypt 31:38
That's a good analogy.

Mário Yaksetig 31:41
David has... it is was so funny. Like, I literally still have hedgehog... like little toys, like fluffy toys that he sent to me while we were working on VoteXX. Just for fun, because he found them on Amazon. It was like a sale, and he sent them to me. So that's where the the hedgehog thing comes to play. And I think it's a great contrast, right? Because it's something that in nature is very simple, but it's actually very effective. So he was always very obsessed with this notion of a hedgehog.

Mário Yaksetig 32:11
And let's go over very quickly, what VoteXX is. So very simple - you have your phone, you have a crypto wallet, and you can vote either yes or no. So for example, they want to reduce taxes, you say you vote for yes or no, like binary choice. And this can then be extended to multiple choices, multiple candidates, whatever the election actually is. So what you do - and this is completely backboned by the XX Network, like the backbone of VoteXX is cMixx. VoteXX depends on the XX Network and cMixx to work.

Patcrypt 32:51
Excellent. So that's, that's number one.

Mário Yaksetig 32:53
Exactly. Yeah, exactly. So what that means is you go on your phone, and that's what we'll be doing for the VoteXX grant, is you go on a website or on your phone, and you have a wallet, you have a crypto wallet, and you register to vote. And think about this way, imagine you are a member of the XX Network community, you have your wallet, you want to be part of the governance process as you should. But you don't really want to just sign your vote and post it on the blockchain, because then again, you will be exposing what the person voted for. And you don't want that to happen, you want the ballot to be private.

Mário Yaksetig 33:34
So what we do in VoteXX is - you generate a key that you're going to be using to vote for that election. And that is very easy to do, you can just generate it from the key you already have. That's very, very easy. And then you, over cMixx, register (you and many other people) register a key to vote for that election. And cMixx kind of takes off that anonymity of who is actually voting. So from there, a couple of people will publish this encrypted public key and then what will come out is just a list of new public keys of people that are allowed to vote, but you don't really know which key belongs to who, right?

Mário Yaksetig 34:19
So if me and 500 other people register, you just know that it's one of those 500 people, so you don't really know who is voting for who or what key they have. So that's step one - that's registration. Then we have a voting phase, so you with a key that is authenticated, (everyone knows that it's a valid key

that you can use to vote), with that key, you vote and for whatever outcome you want. So imagine an XX Network proposal where we're trying to decide between listing an exchange A, an exchange B, we bring that to be a decision made by the community.

Mário Yaksetig 35:02
People then vote using those keys, so we don't really know who is voting for who, like people are just voting, we just know that users are voting for whatever exchange they want. But some of those users may have been coerced. Right? Again, this example, say, I happen to go have a drink with you, and I force you to vote for a specific exchange, and you don't really want that. So what we do is, imagine that same portion happens, then we have what we call a nullification phase.

Mário Yaksetig 35:35
So then, you, a user or someone you trust - that is a hedgehog. So either you or that person you trust, that is what a hedgehog is. The hedgehog can cancel out the vote and they can do so using ZK. And that can even be masked, it can even be a dummy nullification. So then, even if a coercer is with you the whole time, which is a very expensive attack, to perform, like to be with someone the whole time, like the whole day of the election, right? So even performing this at scale is brutal. That other person can nullify the vote for you. Alternatively, if you were coerced, you can then go home and just cancel your vote. And that's what VoteXX allows for.

Mário Yaksetig 36:31
There's a couple of caveats there for it to work. So, if you're very technical, and you're very familiar with the voting space, maybe you're thinking, "Okay, but why don't I force someone to just cancel and then that's okay" - there's a couple of caveats there on how we handle that, we can handle that very well. But we basically, now make it such that coercion is very expensive to perform, and it's not even unfeasible. And it won't really incentivize bribery, because I could pay someone to vote, and then that someone could just cancel the vote. And they would just make free money. Right? That's the I don't even get any downside. It's all upside.

Mário Yaksetig 37:15
Both theoretically or game theoretically, if you were to think that way, malicious actor would not be incentivized to bribe anyone with this, this construction. So this is something that Worldcoin wanted to explore - kind of like the use of a new voting scheme or something along those lines. Because Worldcoin can achieve something very interesting. They can achieve 'one person one vote', because you can actually scan your eye and then you have one key.

Mário Yaksetig 37:45
So when we talked with them, it was very interesting. They knew their stuff they had, they knew of a couple of different alternative voting schemes. And I was telling them why VoteXX is better. And they were super in. So they're very curious. This is actually like, very interesting, this one in the grant application, because then we have shared documents between each other because this is the whole process. And (every member?) in VoteXX is literally... application of it looks great, let's make this happen. But this is a very exciting project.

Patcrypt 38:24
And at the end of the election process, the person voting can absolutely verify that their vote has arrived and is the right thing?

Mário Yaksetig 38:32
So anyone can check that the vote was properly cast in the blockchain. And then you can universally verifiably check that the number of cancelled were properly removed from the tally. So if 100 People nullify their vote, you can check using the zero knowledge primitives that the actual subtraction was correctly 100.

Patcrypt 39:04
So fundamentally, this technology could replace a lot of real world elections.

Mário Yaksetig 39:09
Oh, 100%. So one of the things I can't really give a lot of details here, but we are trying to explore this with a country.

Patcrypt 39:19
A whole country?

Mário Yaksetig 39:21
Yeah, so Exactly. And they. So the way this would be rolled out is we would be running a small pilot first. So conducted kind of like, study group, say, 100 people in a big election vote this way. Then we gather results, see how we can improve the how we can make things better, etc, etc. And then this could be rolled out progressively.

Patcrypt 39:47
Well, that's a very exciting thing to hear, because I did. I did see in your development, your research update that you did in December that there was the possibility of a trial of a real world election so I pondered whether that was to do with this project. So no it's separate. And that sounds enormous. In terms of its scale. Yeah.

Mário Yaksetig 40:08
Unfortunately, unfortunately, the problem is that the election that they're having is too soon.

Patcrypt 40:14
Oh really, that's a shame.

Mário Yaksetig 40:18
Yeah. Otherwise, I think we would be game on.

Patcrypt 40:22
Well, you can still talk to them and test it, I suppose.

Mário Yaksetig 40:25
Oh, absolutely. Exactly.

Patcrypt 40:28
So yeah, it's all it's all go on that. That's, that's really exciting stuff. I guess, you know, some of this technology has been in the pipeline for years that even predates the XX Network. So the fact that it's being brought into the XX Network is just another bonus in its own right, isn't it?

Mário Yaksetig 40:46
Exactly.

Patcrypt 40:47
What, what comes to mind looking at and hearing everything you've just said is that this sounds like a lot of work. But all three of these projects?

Mário Yaksetig 40:59
Yes!

Patcrypt 40:59
Presumably with the grant and the fact that Worldcoin seems to be going up, it means that you should have access at least to some amount of development resource, not just you working your fingers to the bone helping out, doing all the work. How do you see that panning out in terms of timescales for these things? And are they all sort of islands of development? Like do they do they have... is there any dependence on any of the other projects in order to complete one? Or can they all be done in sort of a siloed fashion?

Mário Yaksetig 41:31
So they're all independent, and they are all pretty much independent in a team aspect as well. So we kind of divided and conquered here, we're gonna go with a divide and conquer approach. So we have different people assigned to different projects, actually just had a an architecture call about VoteXX earlier today and things look very good. A lot of integration with the WorldID API and the WorldSDK are starting to happen.

Patcrypt 42:02
Wow.

Mário Yaksetig 42:03
Timeline wise, this is actually somewhat agreed with Worldcoin. So most of these, so two of the three projects will probably be done within three months.

Patcrypt 42:14
Wow, ok.

Mário Yaksetig 42:14
And then the other one is in up to six months.

Patcrypt 42:18
Okay. Wow, that is a lot sooner than I imagined.

Mário Yaksetig 42:23
Exactly. Yeah. Yeah, we're, you know, one of the favourite expressions of David is "Cooking with gas." He always says that when, like development is, is happening quickly. So I think it's an appropriate expression for this situation.

Patcrypt 42:35
Well, this is great. It gives me something to write about as well. I'm always enjoying, you know, trying to get information out of people like yourself to write an article say there's going to be an awful lot coming out from you guys, in the next three months by the sound of it. Absolutely. Awesome. Echoexx has a couple of surprises planned as well.

Mário Yaksetig 42:56
There's a lot going on. Yeah. And I think our community will be very happy. Yeah,

Patcrypt 43:01
There's loads going on. This is great. It's all ramping up.

Mário Yaksetig 43:04
Yeah.

Patcrypt 43:05
And like I say, I guess, you know, I don't know what the mechanics are for you to actually have your hands on the grant funds to do the development, but presumably, you can bring on if this if if your grant money some sometime in the future is worth an awful lot more. There's just extra resource isn't there for the network at that point?

Mário Yaksetig 43:23
Exactly.

Patcrypt 43:24
Yeah, it's a very exciting time.

Mário Yaksetig 43:28
Yeah, the goal is then to also kind of like move on with specific integrations with Worldcoin. So these projects will be completed in again, three to six months. But that's not to say that it will be fully fleshed out and integrated with Worldcoin at that time, right, we will have an idea of what the performance looks like, we'll have an idea of where we can improve. And potentially, we can then have follow up grants and keep doing great work.

Patcrypt 43:56
So on their part, there's no kind of commitment to say, you know, everything you do, we're going to put into our infrastructure. But everything that you do, do, they are definitely going to take incredibly seriously. And, you know, one

Mário Yaksetig 44:09
For sure, yeah, for sure

Patcrypt 44:10
...to pursue it further. And it's just time yeah, time and I'm sure they've gotten, you know, a development strain with all of the other projects that they've given grant money to as well in terms of paying attention to every single thing that's going on it must be like juggling a lot.

Mário Yaksetig 44:26
That's that's a perfect way to put it.

Patcrypt 44:29
Yeah. Well, that's why it's all so exciting and I think the community a very excited by it as well. I was surprised because of obviously then when I first encountered Worldcoin, I was sceptical about the privacy aspects. And of course, once I started reading their website and seeing how, how detailed they'd gone to try and you know, convince everyone that they're serious about it that it kind of makes more sense how much of a shooe-in the XX Network is to them. So yeah, it feels like a match made in heaven like you say.

Mário Yaksetig 45:00
It is and they'll just say something very quickly. This is a fun story. So, a couple of months ago, David and I had already explored Zanzibar substantially. And David always thought of Zanzibar as a perfect fit for Worldcoin. And then fast forward to today, we actually got a grant from Worldcoin to, like, integrate Zenzibar.

Patcrypt 45:26
Because it's I think that was the very first use case you suggested. when the cMixx+ paper came out was Worldcoin, at that point I presume you hadn't applied for anything?

Mário Yaksetig 45:34
And we had no clue of anything. Yeah, exactly.

Patcrypt 45:37
Yeah. So it fit very well. Yeah. Well, that's perfect. I really appreciate your candour and everything that you've said, it makes everything that much more clear. And I'm sure that if there's developers listening, and they're, you know, excited by what they're hearing as well, this is, you know, it's the perfect time to also, we, the XX Network has its own grant programme, I should stress that there is a call out at the moment for different research and development projects that people could bring to the XX Network using cMixx or other technology in XX.

Mário Yaksetig 46:12
Exactly. I'm one of the committee reviewers. So I've read every single grant application so far. It's very exciting stuff we have on the pipeline on that front as well. And if you're a developer, feel free to reach out to me as well, if you want to help out with any of these projects, or some of the stuff we have internally happening. I'm very happy to open it too...

Patcrypt 46:20
Yeah, the more than merrier, basically, when it comes to developers.

Mário Yaksetig 46:37
Exactly. Absolutely yeah.

Patcrypt 46:39
They are definitely in short supply, the good ones.

Mário Yaksetig 46:43
Yes.

Patcrypt 46:44
Right. Well, I'll wrap it up there, but that's been brilliant, and probably the longest transcript I'll ever edit in my life. Maybe not actually, I've done a 2 hour one thinking about it! But yeah, I really appreciate your time, Mario, that was excellent and good luck with the starting of it. Is there anything that's a priority to you in terms of, you know, the pipeline for this stuff? What's going to be on your radar immediately, or is it is you more Echoexx right now, because that's got another Alpha coming out?

Mário Yaksetig 47:14
Surprisingly, I'm not super involved with Echoexx. That's, that is a BitFashioned baby. But it's not my own. It belongs to the other two co-founders and some other team members we have. Right now what I have really high hopes, especially the development speed is for VoteXX. The team we have working on VoteXX is very experienced with web applications, making it fun for users. So I think we're gonna have fun, usable app. And that's the exciting part.

Patcrypt 47:49
Cool. Well, I look forward to hearing your progress of that. Yeah, brilliant. Well, thanks very much. I'm sure it won't be the last time we speak. But we'll, we'll speak again soon and thanks again.

Mário Yaksetig 48:04
Thank you so much. Have a great day.

Patcrypt 48:07
And you bye bye.

Mário Yaksetig 48:10
Bye.

Patcrypt 48:10
Bye.