David Chaum and Jim Dolbear

Talk to Burak Kesmeci about the XX Network

Mon, Apr 08, 2024 6:00PM UTC • 35:58

SPEAKERS
David Chaum, Burak Kesmeci, Jim Dolbear, Haluk Tatar

Burak Kesmeci 00:00
Hello again, David, let's start with you, if you like. Can you please tell us who is David Chaum? How would you describe yourself in two sentences or two paragraphs?

David Chaum 00:11
So, in the early 1980s, I had realised how important privacy would be in the upcoming informational world. That was before the web. I invented privacy protecting technologies to help protect privacy when the digital world would arrive. So those were blockchain, eCash and mixing.

David Chaum 00:53
And then I learned that the National Security Agency had forbidden any conferences on cryptography. And so I risked spending my life in jail, to organise a conference on cryptography where some of this work was presented. And that ended up setting cryptography free. And after that, I also launched Digicash, the eCash company in the in the mid 90s. And its product, you know, its untraceable electronic money was issued by a number of banks around the world. And then I founded the XX Network.

Burak Kesmeci 01:52
That's great. Now, let me ask you, which of the projects you have developed are you most proud of?

David Chaum 02:02
Well, you know, I've done some fundamental basic science work that I'm quite proud of. But in terms of a development, I believe that the XX Network, which I founded has the longest life of my software projects I've founded and it's quite stable and active, and it's got a really great community. And so I guess, I have to say, I'm most proud of that.

Burak Kesmeci 02:39
Okay David, what is XX Network, and how long will it take for the quantum computers to become widespread, and is it dangerous for the cryptocurrencies?

David Chaum 02:54
Well, few people seem to really understand this issue. And the facts are, that probably, governments will have quantum computers before other people do. And they may wish to take down blockchains. And if so, currently, there is no blockchain that I know of that would withstand that kind of an attack. We, however, have been building (and we demonstrated) the version of a new consensus algorithm that runs very fast and does withstand such an attack. But we have not completed the project to move over to it.

David Chaum 03:54
Okay. There's a second kind of attack on a blockchain with a quantum computer. And that is that someone could basically make false transfers. So they could steal your money. And it's a little more difficult in some chains than others, because in some chains, as you may know, the actual public key is not public until you move some value from that wallet ID. But it doesn't matter, this is certainly an issue. And yeah, I guess that's enough said right there.

Burak Kesmeci 04:44
Okay, David, I'm with you again... Asked a question about notary systems. He told that you worked on notary systems - election systems in fact. So will XX Network help us about election systems in the near future, or for the future?

David Chaum 05:10
Oh, yes. But I think we should talk about quantum computers again, cos there's a little more to the story. But we have a project now to implement an election technology that we developed using XX Network. And actually, it's a grant. I think, Jim can speak more to that. But, you know, we've been engaged in a kind of academic research project, although we've made some code over a couple of years. And we found some very fundamental, important results in election technology

David Chaum 06:00
And essentially, what it amounts to, is that cryptocurrencies can be used to destroy elections, by kind of bribing people to vote a certain way. However, with this new breakthrough that we've made, and which is now being built, (and will use XX Network) it's not possible for a vote buyer to learn how you voted. And this is an extremely effective, and the only known solution to this problem. And so, it's my belief that voting outside of polling places and more frequent voting on different subsidiary issues, will greatly strengthen democracy, and is probably needed, because of artificial intelligence and the complexity of modern society.

Burak Kesmeci 07:10
Now, I have different question. Recently, Vitalik drew attention to the quantum trends. Did you have any discussion on this topic with Vitalik, or some specific person on the topic?

David Chaum 07:22
You see, XX Network has done two things to protect our community against a quantum attack. One of the things is we have a quantum resistant consensus, which we demonstrated - we ran it for 10 days. And it's not yet integrated in the chain but it worked, and it worked very well. (And that was public, on YouTube, and so on).

David Chaum 07:57
The other thing we've done is, we have built into essentially every single XX coin that anyone (key) that anyone would have, actually has a quantum secure signature built in beneath it. So there's a quantum secure signature, which is a fallback. And then it actually signs a... it actually is a preimage for a public key, which is currently used by the holders of XX coins. So, we published this in a series of four articles now, already starting a few years ago. And so as far as I know, ours is the only chain that has anything like this, we created it. And it's been quite well known for a number of years. And I think that Vitalik has made some comments, which, in my opinion, he borrowed very heavily from what we... basically he claimed that he had accomplished what we already had published several years ago.

Burak Kesmeci 09:40
(thanks again, David)

David Chaum 09:45
It's a little more complicated than that, but I can tell you more about like...

Burak Kesmeci 09:50
Okay David, this is this is the other question. You have recently announced that you have a cooperation with Worldcoin. What is it for?

David Chaum 10:06
Well, I'm not sure. I mean, I'm the founder of XX Network, but I've not actively, you know...

Burak Kesmeci 10:17
Okay, then I'll ask the question to Jim

David Chaum 10:20
Jim would be the best person to ask about that. Yeah. He's very familiar with the details. I just want to say that, yeah, it's a little bit embarrassing when, you know, Vitalik claims to have invented something that we've already published over years, and we created an open standard for it, and we built it into all of our keys. So it may very well be that what he proposed only works for keys that have already been used previously. If a key has not been used, when a quantum computer is built, then I think that the quantum computer could steal that key, and that what Vitalik proposed would be ineffective, but that is not the case. I'm not 100% certain about that. But in any event, that is not the case for the Sleeve technology, which XX has built into all the keys and is published.

Burak Kesmeci 11:26
Okay, now, David, we can start talking with Jim, I have some questions, Jim, for you. Who is Jim Dolbear, can you please introduce yourself to us? And I believe you studied at Harvard, right?

Jim Dolbear 11:42
I studied economics, which is the decision making by businesses on pricing of their products, how much of the product to make, how to protect themselves competitively against competitive businesses. And also the more macro (that they call macro economic issues) of how does government manage the money supply, including inflation, central bank activities, and then also the whole issue of regulation, and the design and implementation of public policy to prevent things like monopoly, (private companies

controlling markets) which is a big thing in Europe now with Google and Apple and Facebook. And also things like providing public power and water and how to set prices for regulated utilities.

Jim Dolbear 12:49
And then I also studied religion, there is a divinity school, which is a religious school, a graduate school at Harvard. And I was part of a programme to compare religions around the world. And then after I left Harvard, I took the background in economics and finance and I worked in New York, at two top 10 investment banks, Morgan Stanley and Lehman Brothers.

Burak Kesmeci 13:27
Now I have the next question. As the CFO of XX Network, can you tell us two of the features that set apart XX from the other crypto projects?

Jim Dolbear 13:42
Well, to start off, I'm actually not the CFO of the XX Network. And let me clarify because it helps to answer the question. XX Network is a decentralised project. It's controlled by on-chain governance and supported by a Foundation. The original software was developed under David's leadership through a Cayman Island Company called xxlabs, and originally through a United States company called Privategrity Corporation, and I was the CFO, (or am the CFO) of Privategrity Corporation. But all of the work that Privategrity Corporation did, including the work done by xxlabs in Cayman Islands has been transferred a year and a half ago - actually two years ago when we went main net to the network itself - to the coin holders supported by the Foundation. And I am a board member on the Foundation (David is not) and I'm a member of the operating committee for the Foundation, so I do work for the Foundation.

Jim Dolbear 15:04
Okay, so what makes the XX Network distinctive is that it really is a decentralised network. It really is. And let me give you more detail. There are 360 different nodes around the world in 60 or so countries. And those nodes are controlled by individuals, not by corporations that are US based, not by venture capitalists, but by people around the world. And those nodes run the XX Network software, which is two pieces, right? There's a blockchain, like other tier one, projects. But we also have cMixx, which is a mix network. And it's an accelerated mix network. So it's a very fancy version (and a more efficient version) of what David invented in the early 1980s, a mix network to provide privacy so that your activity could not be traced online.

Jim Dolbear 16:18
So we have, at the XX Network, a privacy layer that no other blockchain has, and we are truly decentralised. And we are proof of stake. So the blockchain, the project, is controlled by people around the world. I don't really want to allege this too much - but many of the projects that are most famous are in fact controlled out of the United States with large shares of coins and control in US venture capital firms. So we avoided that, we deliberately on purpose did not want to be US controlled, we only have one US investor originally. Now it's hard to know who owns... you know, because the coins have been traded publicly....

Jim Dolbear 17:15
But there's only one US investor from the beginning and that's Chris Larson, who founded XRP (Ripple). Other than that, we never had any institutional participation from venture capital firms early on, and that's very different from most other projects. So, you know, we are really decentralised, we really

have nodes run by actual people. We really don't have US venture capitalists controlling us. And we really have a privacy layer, which is unprecedented. So those are the three.

Burak Kesmeci 17:53
That's great, especially I truly appreciate that you're, focusing on being decentralised. I mean, truly, we all know that 99% of the projects that claim that "We are decentralised", but they're always run by people or venture capitalists, which XX doesn't have. That is great.

Haluk Tatar 18:17
So may I ask you a question, please?

Burak Kesmeci 18:20
Definitely.

Haluk Tatar 18:21
How do you see the impact of countries and governments on the future of cryptocurrencies? I mean, not only Bitcoin, my question is about your XX solution. At the same time, you will say that it's possible to keep the freedom of all kinds of digital currencies (we know 10,000 maybe right now) they could replace existing dollar, euro currencies away from many countries. So I mean, domination of USA or domination of China on cryptocurrencies, they'll be interrupted by XX. So XX system will be a complete solution against to this domination, right?

Jim Dolbear 19:09
Yes, I would answer the question (and I go back to what David said) that when he said he remembered and described how he had founded the International Association of Cryptologic Research. He said that he set crypto free. Technically, what happened was a entity, a nonprofit entity was formed under the United Nations for all people around the world to share cryptographic or cryptologic research. So the first answer your question is "Who controls cryptography?" The actual research and protocols and because of the work David has done, the United States does not have control of cryptographic protocols, the way they wanted to do in the early 80s. So that's one answer. Now, that said, David also said, that countries (and there's maybe five or six extremely sophisticated countries) have deep understanding of cryptography and are developing quantum computers.

Jim Dolbear 20:23
So that's why David used the word "attack". If those state actors, those countries have quantum... when they have quantum computers, they will be able to attack all the chains that do not have quantum ready signatures. So that's a point of attack, where if your chain and your currency does not have quantum resistant or quantum ready signatures, then these countries can attack you and take you down. Then the other piece of it is what I was alluding to, which is, where the nodes are, and where the... and how each blockchain or project is actually managed, creates an exposure to kind of a legal attack, which is what you've seen in the United States with XRP, and Ripple.

Jim Dolbear 21:21
So if this is why if all your nodes are in one country, there's a problem, because that government in that country can attack your nodes. But if you have nodes everywhere, all over the country, it makes it very difficult. So basically, it's decentralisation of cryptography, which is what David started with IACR. It's using quantum ready and quantum resistant technology so that the rich, powerful governments with

quantum computers can't attack you. And it's really having true decentralisation of the nodes and governance, so that you can't be attacked sort of legally. Those are the things that are critical.

Burak Kesmeci 22:10
Okay, David, sorry, Jim. There are a lot of people in Turkey wondering, "Will XX be listed on other exchanges soon?" Now, you are listed on MEXC, right? Will we see you in another exchange soon?

Jim Dolbear 22:36
So, yes. First, the reason we listed on only one exchange, originally at main net was because we wanted to list the native coin for the security of the network. So, with the native coin, the nodes can be staked all around the world, and it secured the network. So that is why we started with listings of the native coin, because it was critically important to the security the network. But that made it difficult to list on exchanges, since most of the coins that are listed on exchanges are not really blockchains. They're not tier one, they don't have nodes, all they are is a smart contract, right? So most of the exchanges list, basically Ethereum, wrapped, smart contract based coins. And so it was hard for us to list the native coin on other exchanges.

Jim Dolbear 23:45
That said, this weekend we listed on Biconomy. And if you go to CoinMarketCap, you will see that, so we're now on two exchanges. But the listing on Biconomy is the wrapped version of XX. So it's not the native coin. And it's called WXX. It's wrapped, which means you can hold it in Ethereum wallets and it can be part of the Ethereum ecosystem. And we're also going to list on a smaller exchange, which is not very well known called Coinstore. And the reason we did that is that Coinstore was founded by some younger Asian people during COVID. So they're very community based and they're trying to grow and they're small, so we wanted to partner with them.

Jim Dolbear 24:41
So we'll have three centralised exchanges very soon. MEXC and Biconomy exist and the coin is tradable right now, and Coinstore is coming soon. Another important part of that is that CoinMarketCap which is the official sort of listing, third party data... you know, publishing app and website for the crypto community will not verify your numbers unless you have three exchanges.

Jim Dolbear 25:16
So a real goal for us was to be listed on three exchanges. So that CoinMarketCap would verify all our information. And then the next step, which is part of the work we've been doing for months on creating the wrapped WXX coin, and a bridge between WXX and the native coin XX is we're going to list on Uniswap. So that will be a decentralised (obviously, it's Uniswap) a decentralised listing, if you will.

Burak Kesmeci 25:51
Okay, David, we have some questions. Sorry, Jim, where some questions for you. You have recently partnered with with Worldcoin. And both XX and Worldcoin have seen significant gains in value. What kind of contribution did you make to Worldcoin?

Jim Dolbear 26:10
Well, let me answer that on behalf of the XX Network. But I'll also share some information about what some of the other members of the team are doing, including David. Concretely there are three grants, (wave zero grants) which were given to projects that are associated with the XX Network, to help look

at solutions for Worldcoin to address their privacy problem. And the first is to provide them with easy to use integration tools. So they can use the XX Network, and that is the "XX Network" grant. And what they want to do is have easy access, so that people who use Worldcoin and the Worldcoin ecosystem can easily send data and messages through the XX Network, so that their metadata can't be collected and their activities can't be tracked. So that's the first grant and that is the "XX Network" grant. And if people want to see their brief descriptions on the Worldcoin site of the 'wave zero grant programme', so you'll see it's only a few sentences, but you'll see these grants described.

Jim Dolbear 27:35
The next one is a project called Zanzibar. And it's under David's leadership and Mario. Baltasar is also working on it. Mario is one of the original team members. And Zanzibar has to do with the way Worldcoin handles biometric data, which is to say, they have this thing called an orb, which takes a picture of your eye. And what David has done is designed a way so that there never is an actual image of your eye, it's immediately turned into an encrypted code. And this is critically important because it prevents the notion that Worldcoin has a database of images of everyone's eyes. And that is called Zanzibar. It's under David and Mario's leadership, and that, too, is described on the Worldcoin website.

Jim Dolbear 28:35
And then the third, which David actually mentioned (I think you asked the question about) is VoteXX - anonymous, secure online voting and Worldcoin is interested in using that for governance. So they gave VoteXX also a grant. So those three grants are the grants that you'll see listed on the Worldcoin site under the 'wave zero' grant programme. And there are other grants, I think there are 20 in total, but no other kind of group had three grants. And I think what Vitalik had said (mentioned) that people are seeing that Worldcoin is trying to be active in addressing the issues that have been raised about privacy, and part of that is giving us these grants to explore how we can help solve the problem.

Burak Kesmeci 29:36
Okay, Jim, I have one last question. Then I am going to ask another question to David. Do you plan to collaborate with other projects besides Worldcoin?

Jim Dolbear 29:51
For sure. Right now, we're working with a number of the major wallets to integrate both the native coin, (the XX coin), so it can be accessed directly. And then as part of echoexx, which runs on the XX Network and protects people's metadata, (but is a more general purpose hub for W3. and for participating in the Ethereum ecosystem) you'll be able to use WXX, the wrapped version of the XX Coin. So those are two things we're doing to integrate financially. And then additionally, there are a number of partners who, like Worldcoin, are looking at using the XX Network to run traffic on a wholesale basis to protect that traffic from activity tracking or metadata collection.

Burak Kesmeci 30:59
Thank you. One final question I have for David. In the near future, we can see quantum and AI working together and a couple of weeks ago, we have learned that Apple created a system for defending quantum attacks. And what is more, IBM is right now building a quantum computer. And what will we have to face in the near future, about quantum attacks?

David Chaum 31:34
Quantum attacks can break all kinds of crypto... cryptography, I should say, that's used today, which is based on so-called public key cryptography. And, in fact, most cryptographic systems today use public key cryptography to a certain extent and therefore they are vulnerable to such breaks. Various government agencies have asked people to switch to different kinds of public key cryptography, which is secure against quantum computers. Now, this is pretty easy to do. But it is not guaranteed to be even better than what we have today.

David Chaum 32:30
And that is because there is no proof that these systems are not easily broken by ordinary computers. So they look interesting, there are new kinds of systems, but we don't know how secure they really are even against regular old computers.

David Chaum 32:53
You know, the history of government agencies is that they mainly have (over and over again), recommended that people use certain kinds of cryptography. And then they themselves do not use it. And it turned out, over and over again, that those systems were breakable. So if you go based on history, you have to assume that governments are telling people to switch to a kind of cryptography which they can somehow break, because that's what they've done over and over and over again. So they're using the idea that it's secure against a quantum computer, but it may not even be. So this is...

Jim Dolbear 33:42
Can I... Can I interrupt and just point out, David does not work for a university, in the United States, or anywhere, and he doesn't work for the US government. Everyone else does, pretty much. And so much of the cryptographic research is done through grants from the United States government. So this is part of the problem. The US government has a lot of control over these supposedly secure cryptographic protocols that they develop. So I think that's - I'll go and say that - so when a centralised entity, like the US government tells you "We've paid the scientists, we've worked to develop these protocols. They're very secure." You have to think twice about whether or not that's completely true.

Burak Kesmeci 34:37
Okay. Now, let me sum up all the talks and we'll finish it. And because I know you're going to go to Paris tomorrow, so I don't want to take too much time off yours.

Jim Dolbear 34:56
Very sensitive of you.

Burak Kesmeci 34:58
I do really thank you. And David, I described you as the father of the cryptographic - like Oppenheimer is the father of the atomic bomb, so everybody can understand who you really are. And Jim, I have I have described... I don't know how to describe you, but you have already introduced yourself perfectly. Especially... you're graduated from Harvard and worked at Morgan Stanley and the other bank that I forget about, I'm sorry. I have taken at least five pages of notes, and I do really appreciate you sharing time with us. I know that you're going to go to Paris tomorrow, and in front of all of our listeners, I do thank you.

Jim Dolbear 35:52
Well, we thank you.

David Chaum 35:54
That was a pleasure, really. Thank you very much, everyone.