Bitcoin Olympics Hackathon Launch X Space - David Chaum Speaks About Privacy and AI

Monday, August 5th 2024 5:00PM UTC

SPEAKERS
Melanie Mohr, Edy Haddad, David Chaum, Adam McBride

Edy Haddad 00:00
I see David is now a speaker with us here on stage. Hello, David. I'll leave the floor right now to David so he can say hello to us. Give us more introduction. Been a while since I heard his voice, and I miss it a lot.

David Chaum 00:14
Hey, Edy, nice to hear you. Well, Edy, don't be fooled with that. Edy and I worked together on a number of things, and we had some nice in person meetings, and now we mostly communicate remotely. But, yeah, I was just asked to give some basic background here. And because the judging isn't coming up for a while.

David Chaum 00:43
So I'm happy to try to evaluate… the contestants. And I totally agree with Mel that, it'd be really, really great to see some good stuff built on top of all this. Many of… just a real quick background that in the late 1970s I realized how important digital technology would be for ordinary people in the future. (can everyone hear me?) Okay, yeah, and anyway, so I started trying to figure out what would happen moving forward, and I realized how critical privacy was to the choice between whether it would be a web2 world or a web3 world in today's terminology. In other words, would companies and government in a centralized way, kind of control people through digital technology, or would people be empowered with their own computers and, well, I realized keys to protect their own interests.

David Chaum 02:07
And so, there's a big, big difference there. That's something I felt very strongly about. I wanted to sort of save humanity and try to steer things in the web three direction. So I, excuse me, spent a bit of time trying to figure out how people could protect their informational lives in a digital world. And this is when I realized that cryptography was the key, no pun intended - was the way to do it, only way to do it, in fact, the only way to create real structure in a digital world and to allow people to enforce protection of their own information, their own rights, their own privacy, money and so forth.

David Chaum 03:09
And so that's when, in the end of the 70s and first year or so of the 1980s, (this is way before the web or anything), I figured out how you could do mix networks, which is what XX Network does now, and this is, (excuse me), as I'm sure many of you realize, the way to protect the privacy of basically who communicates with whom and when, so messages are routed in a… the internet is the packet switching network, and mixing could be built in, but currently, it's only an overlay, and you can thank the National Security Agency and their various contractors, like BBN for that. Go back and look at the original RFPs, I'm sorry, RFCs, in the early days of the Internet, Internet Society, you can see all this stuff. And the chairman of the privacy working group was an employee of BBN, which is a military contractor in Boston. And he wrote in the introduction that under no circumstance could cryptography be used to protect the privacy of header information.

David Chaum 04:48
That's what Steve Kent wrote while he was being paid by the National Security Agency, and put it in this public standard. Can you imagine that? Have you ever seen something like that in an RFC, where it would say, what you can't do. It's supposed to tell you how to make interoperable standards, not say no one can ever do this, right? But it's what it says. Go look at it. Thanks to the NSA. There's… and people try to bring this up subsequently, and it was always shot down very energetically, really, mixing should be in at the protocol level of of the IP stack, the routers should allow mixing. They should allow the encryption of header information, but they don't.

David Chaum 05:44
So mixing today is only as a so called overlay on the network, which, of course, makes it much more expensive and slower, and you have to try to get people to use it, and so it's not very widely used, but it is increasingly used, and that's great news. I'm not here to promote XX Network, but you can have a look - the Foundation is making a lot of progress. They're getting a lot of different kinds of uses, use cases to run over the network.

David Chaum 06:24
So that was one of the things I came up with, was mixing and the other thing was blind signatures for untraceable payments like so-called Ecash and what I think most people aren't really aware of or recognize that actually it's just a generalization of Ecash, strictly speaking, what I've called like in the Scientific American article, which you can find a copy of on my website, chaum.com, where I lay out how you can combine mixing for communication privacy with Ecash for payments privacy, and then what I call credential mechanisms, the generalization of Ecash for all kinds of personal information, where you would basically keep the database of information about yourself in the form of signatures by government and organizations that were issued to you, and then you could prove various assertions about those in so-called zero knowledge or minimum disclosure, something which I had a lot to do with creating, but that's a story for another day.

David Chaum 07:42
And, I think it was Henry Kissinger, now deceased, who said that "Academic fights are the most bitter, because there's so little to fight about", he said. So okay, I had a lot. I invented a more general notion than zero knowledge, the one that includes snarks was so-called minimum disclosure. I showed how they are duals of each other. The more general result, how could they all be reduced directly to circuits, but certain people in the field who are still with us tried to cover that up and pretend like it was all about zero knowledge, and that was the whole thing. So that's really a travesty, but any event, so, but just

when I was starting to see the light at the end of the tunnel, how these protocols could provide privacy, there was a glimmer of it. I was quite enthusiastic about pursuing this.

David Chaum 08:47
The National Security Agency got a new director, a new head of it, and this guy said that it was his opinion that anything to do with cryptography was born classified, and that if you...sorry about that... you had to keep it secret. And so if you organized a conference about cryptography, then he was going to put you in jail and, like, throw the book at you, the whole weight of the federal government at you. And he said as much in letters, which he wrote to the IEEE and the ACM and so on. And this was reported in Science Magazine. You can read about it on my chaum.com under the IACR panel, because what I did was, of course is what a good Berkeley graduate student in cryptography who saw how important it was going to be for for protecting people from government in the future, would do - start a Conference on cryptography.

David Chaum 10:02
And fortunately, I didn't end up spending the rest of my life in jail, but I did, found the International Association for Cryptologic Research and announced it at that first conference. And so that has the backing of the UN and all this, and you can read of all about it and the reporter who broke this story in Science Magazine, by the way, has a funny name, which is easy to remember. Her name is Gina Colada. Okay, I haven't seen her doing much recently, but so anyways, she wrote about this, and no one could believe it at the time that the government was trying to make cryptography be born classified like nuclear weapons. But there you have it. So that's pretty much. And then I had a lot to do with the cypherpunks, and inspiring them. And I spent a lot of time working on this kind of thing and going around giving lectures about it at universities, and the articles were published in major journals. What was the best journal computer science at the time, ACM, appeared there on the cover then it later invited Scientific American and appeared there in a more abridged, edited form, in, I think, 12 languages. And people love this whole idea that that you could control your own information and through cryptography by basically keeping everything private using mixing untraceable electronic money and credential mechanisms.

David Chaum 11:44
So it's kind of a comprehensive solution and so, but a lot of the people you hear about in connection with Bitcoin were my friends and colleagues, and I hosted a lot of visitors in Amsterdam at our offices, Digicash, where we issued Ecash, our own cyberbucks, like Bitcoin, right? And then we also had licensees like Deutsche Bank, which was the largest bank in Europe at the time, and other, was available in issued in US dollars and a number of other currencies by various banks around the world. So that was pre-Bitcoin, and it wasn't fully decentralized. But I don't feel guilty about that because of two things.

David Chaum 12:41
One, there wasn't enough computing power really to decentralize it fully at that time, and we had trouble getting it to run on the 386s and 486s that people were using. And the other thing was that we actually spent a lot of time. And this is not, I maybe haven't said this publicly before, but I think I'll end on this. We spent a lot of time, and that's a couple of two of the really key people at digicash, super great, brilliant, young Dutch guys, Yelta and Niels and we would spend hours, many evenings in our… we had a conference room with white boards on like two sides a lot of whiteboard space and big windows and stuff. And we would spend hours in there working on, trying to figure out all different ways

to decentralize this stuff so it wasn't like… we didn't want to, or we… some people said, Oh, well, you could have minted more Ecash. you've stolen Ecash. Well, no, at that time, no one ever said that.

David Chaum 14:03
With Ecash, the cyberbucks, we issued it, and we said we're going to issue only a million dollars worth… cyberbucks worth. That's it. And anyone who opened a shop that would accept cyberbucks, we airdropped them, what you say now, we gave them some free cyberbucks. And if you go to the chaum.com and look at the Ecash panel, you can see the Ecash Museum and all a lot of the shops and see what they were selling and stuff through this, a lot of it is reconstructed through the Wayback Machine. So it's not all there, but quite a bit of it is there. If you hover over the icons of the shops, and click through on their names, you'll see some of their web pages and what they were selling. And so that was the cyberbucks system. So we actually had quite a lot of... people realized how important all this was going to be okay. I think I've burned up my airtime. And thanks for listening. It's a pleasure to be here. Thank you,

Melanie Mohr 15:10
David. Thanks so much for joining us here, and also, supporting us here in our journey. It was, yeah, a year back, I think, I mean, we met at one of the Satoshi roundtables and then reconnected in Dubai. And yeah, was a great moment for Edy to be introduced to you. And even greater, after a few calls that we were able to convince you kind of to support us. And we are very, very thankful that you are helping us to to build what we are building now with Pwrchain.

David Chaum 15:48
Thanks Mel. And when we met you and I met a couple years ago, I was very impressed by the way the projects that you had been working on, and what you described and and so on. And that's really, yeah, what motivated me to say, we all would like to continue to back you and, yeah, it's, it's been fun working with Edy on some of the real tricky inner details. That's, kind of stuff I do just for fun. So it's been good. Thank you very much. It's really great.

<Unknown Speaker> 16:25
No, thank you. Thank you for being here.

Edy Haddad 16:29
Yeah, I just want to say it's been a pleasure working with you, David. First, I was very happy that I was able to have had to had conversations with someone like you. It kind of gave me big satisfaction that I'm on that level where I can have head to head conversations with no problem. I can understand everything you're saying, and go along with it and improve on it together, and all of that. So it was very satisfying and assuring for me on on the level I've reached so far. It's also been amazing working furthermore, on mhbs together. And also another thing, guys, because I don't know if anyone mentioned it, but to those of you who don't know, David Chaum,, as he just said, right now, he's the creator of Ecash, or digital cash was called, which actually Bitcoin took as reference when being built. And David Chaum is one of the most mentioned people in the Bitcoin white paper?

David Chaum 17:28
Well, let's put it this way, Edy, when I made the first e cash payment at the First World Wide Web Conference, which was held in Geneva at CERN, where the web was invented. There were two keynotes, Tim Berners-Lee and me, right. And mine was first. And I made a payment, the first international, Ecash payment, back to Amsterdam, and I wrote a three paragraph press release, sent it back to our amateur PR, part time PR guy in the company, Paul Dennison, and within like 48 hours, There were articles in the New York Times, Wall Street Journal, everywhere, all around the planet, because the smaller publications always follow the bigger ones in those days.

David Chaum 18:17
And it was the idea that a number could be worth money, a digital bearer instrument. That's kind of what I got credit for inventing, and that that kind of rocked the world. And you could say, well, I'll leave it to you any to the list, or here to decide whether bitcoin is on a similar standing or with a relative, that was, that was a very big deal, because prior to that, the only bearer instruments were stock certificates and bank notes and yeah, to make it, be a digital bearer instrument, solve a double spending problem, and actually build it and make it work and everything was, it's kind of kind of a big deal. I think so.

David Chaum 19:10
Anyways, it was really fun and rewarding. We had a great company, like, we went out like these team building things. We rented like, one of these old Dutch sailing ships and sailed it across the eye. And it was just great, great working with all these peoples and, so, (Nick) Szabo, we had him there for a while, and Zooko (Wilcox), who went by a different name at the time, but, he worked there for a couple years, and I just wanted him just to work on his own thing. And so even though we paid him, I just helped him try to figure out a better way to do Ecash than we were doing it. That was this project,

David Chaum 20:04
So that that had that bore some fruit. Anyways. Okay, enough from me.

Edy Haddad 20:12
Now I can imagine that that's definitely what you just mentioned - I'm imagining if I were in your shoes. That's definitely a historical moment and historical times to remember, and anyway, they pushed the way to where we are today. So thank you for all of that.

Melanie Mohr 20:30
Maybe I don't know if, David, I'm not sure about your schedule. I know you're a little bit tied today, but if there are some questions I see...

David Chaum 20:40
I have some some visitors here at my home, and I think I need to talk to them, because they're on their way....

Melanie Mohr 20:49
But Adam, I see he has his hands up.

Adam McBride 20:53
I'll just sneak this one in. David, huge fan. We met at the round table as well one time. And I don't think there's anyone more important in the history of Bitcoin than you. Actually just having a talk today with

somebody who's writing a book, and one of the sections is about Satoshi and contemplating who it is, not saying it's you, but when we're talking about who's important in the history of blockchain and Bitcoin, you're obviously at the pinnacle. Quick question, though, on current state of privacy and blockchains, obviously US Government's going after people who are creating privacy tools. I just wanted to know your current feelings on the matter and and where you think we sit as an industry trying to protect people's privacy.

David Chaum 21:42
Well, Adam, Thanks for the kind words. And that's a question that calls for a pretty elaborate set of issues and discussion points and so forth, but I would say... I hope people don't get discouraged, because there is bad news out there. The so called travel rule, is gearing up. It's coming into enforcement in different jurisdictions, even though it was introduced more than a year ago, but it's starting to actually take force in some places, if you look at what the powers that be are really up to, which is something I know a lot about, because I'm… I do hang with some of these people as well. Don't hold it against me. I mean, I have the luxury and freedom to enter a lot of different circles. And I spent a bunch of time at the Satoshi Roundtable, speaking of which at the Bitcoin maximalist sessions, really trying to get into it and everything, and really hear… this all out.

David Chaum 23:31
But so there's bad stuff. There's movement in an anti-privacy direction. It's certainly happening. And , the crazy things have happened, as you all know. I mean, can you imagine putting a developer in jail in another country or something - it's ridiculous stuff, but there are some sort of behind the scenes, countervailing things happening. In the United States. So we have this kind of, like idiomatic expression or vernacular something it comes from the advertising world with billboards. Sometimes the billboards will just say something like, "Watch this space." to mean that that company's probably going to announce something soon, but they can't say what it is right now. So I'd like to say, "Watch this space.' I'd like to say you haven't seen anything yet. Maybe that's a little too strong, but I've got some new stuff that I think can change the debate. It's not just an either or thing. It's a bit complex. And I think there's, there's stuff that can be done, and there's certainly improvements possible at the layer 1. This is something a lot of people don't realize.

David Chaum 25:08
I mean, I was just at a really nice event in Tokyo, with… it was really nice to be there. The people so kind to have me there and everything. But I couldn't really bring myself to say it. I was on stage with Vitalik and everything. But we had this panel, and I just couldn't say it. The plasma people are all happy about trying to make better privacy as a kind of layer 2, an add on kind of a thing. And honestly, if I were to really speak my mind, I would, I'd have to say you cannot build privacy on. You have to build it in. It's the same as with security. You cannot build security onto something that already exists. It has to be architected in from the beginning. Otherwise, it's hopeless. These are hard problems. And, yeah, privacy's… it's, comparable as hard as security, it's a tricky stuff. So, yeah, I'm sorry for the maybe long winded answer, but I think there's hope. And ideas can be very powerful. And it's not just them or us, a cut and dried, black and white issue of privacy or no privacy. It's somewhat, it's, quite a subject.

David Chaum 26:58
I mean, Vitalik commented that there are really no metrics for privacy at that panel. That's not exactly strictly speaking true. And I tried to politely point out that we have developed metrics like anonymity sets and there's information theoretic analysis and various other stuff, but, it's also true that in these

real world applications, it's hard to really get your head around the privacy issues, and all the models and what, what's really offered, what the worst case, what an attacker could really glean, and all the various scenarios and so forth. It can become very complex. So anyways, don't lose heart. There's a lot of room to do some great stuff. And one last, I mean, thanks Adam for this question…

David Chaum 28:03
I guess you struck a nerve here. One more thing I want to add, and then I really have to go... I think we are in a very different world today with respect to privacy, just in the last couple of years because of AI. And so there's two aspects, right? There's the historical damage to civilization that's been done by artificial intelligence, in some of its more primitive forms in web2 social media. It's created a fractionation... it's really done a number on civilization, and that's a horrible thing. And now let me just… I said more, and you could look at some of my presentation, perhaps at the plasma conference. I think it was live streamed, but it's on Twitter and so on.

David Chaum 29:12
So, nowadays, privacy, with AI really represents a much higher stakes game, because to put it... think of it this way, if let's just say, really bad forces, whether they're human or not, get a hold of some portion of civilization, they can use AI to hold on to their power, and that means that they can use robots. And all this stuff and spy on people and brainwash people through AI. And it's really not easy to imagine that we would be able to shake off such a bad form of governance.

David Chaum 30:18
Used to be you just prize some some pavers, some stones out of the street, and start throwing them. And governments would listen, but when they have... they know everything about you, you don't have privacy. And then, they're ferreting out all this information and putting all these pieces together with AI. And then with the vastly more powerful, I mean, humans can't, really, I think, have a fair fight with an AI powered robot with automatic weapons and everything. I mean, have you seen any of this stuff? It's like, super frightening, right? So it's like the balance of power has tipped. If so, if we lose, lose control now, it's not ever coming back, get over it.

David Chaum 31:10
It's not the same old world like we could try these experiments and all we could always claw our way back. No, this is it. It's sort of you only get one chance going forward, and that's because of AI. And the more AI knows about all of us, the easier it is for someone to really use their power. And that's where the privacy thing comes in. But there's, there's more to it. So a lot of the debate has changed because of AI. And, AI can help people, and protect their own privacy, right? Because a lot of these tools that we developed are very complex, difficult to use. What you need is, put this way, and I really will shut up...

David Chaum 31:57
But.... The thing is, in future, if I have a personal AI, it will tell me the products and services to use that are best for me, and if the user experience is the same as the non-privacy ones, it will just go directly to those. So it's not... so the privacy based apps and information services and so on are not going to be at any disadvantage. In fact, they will be favored, and they can expect to receive massive immediate adoption. It's a very different world, you can do all the hype and marketing you want, but you're not going to fool people's personal AIs. They'll figure out what to do, and they'll do the right thing, and they will choose the products that have privacy if the user experience is similar. But that's what AI can also

help with. So the importance of privacy is amped up because of these downside scenarios that I mentioned.

David Chaum 33:11
So anyway, so I look forward to seeing meeting all of you personally and stay in touch through this and and everything. And I think our community is on the right side of all this, and it's, it's a critical, it's becoming all the more critical. So, yeah, it's so great to be here with all of you. So thanks again.

Melanie Mohr 33:36
David, thanks so much for joining us this evening or this morning. Your noon, wherever you are, was very insightful, and we're really very honored that you're working with us and for all the startups that are building on Bitcoin plus they get in front of David for yeah, seeing the projects, judging it. So please join us and join the Bitcoin Olympics hackathon. Thanks so much, David for your time. Was amazing to have you with us.