Craig + Ryan Q&A podcast audio.wav

Ryan X. Charles [00:00:13] Welcome to a special edition of CoinGeek Conversations, I'm Ryan X. Charles, founder and CEO of Money Button. I'm here with all of the participants of CambrianSV in Lisbon, Portugal. And we're very delighted that Dr. Craig S. Wright, Chief Scientist of nChain was able to join us today. Could we all please welcome Dr. Craig Wright? (applause) So we wanted to give people here an opportunity to ask Craig questions. People probably have who knows what types of questions. Let's just give people a chance to ask this. So I want to just kind of frame the conversation a bit and ask you a very, very high level question to kind of kickstart this. Craig, what is Bitcoin?

Craig Wright [00:01:03] That's a very difficult question. At the sort of end, it's a peer to peer electronic digital cash that is an exchangeable token. That token is then distributed and validated with a peer to peer distributed registry.

Ryan X. Charles [00:01:22] OK, so then because we're just talking about SPV and you know, SPV stands for simplified payment verification, if that's correct. And this is in the original white paper. And this is kind of a theme of the history of people involved in Bitcoin. This has kind of been an important concept that, you know, some of us anyway are starting to recognise that the central importance of this for the future of Bitcoin. Can you maybe just explain what is SPV and what is this?

Craig Wright [00:01:48] I've been told many times that I'm not allowed to name anything ever again. And SPV is one of these things that I thought actually was explanatory. But obviously no one else in the world outside of myself knows, knows and understands. So SPV is really the user level network to do with Bitcoin. So after Bitcoin starts to grow and scale which it's already done then to be peer to peer electronic cash, the way it actually mentioned on my original website before everyone changed it and made it the whole core coin thing now, you have peers exchange data and that's what SPV is for. Not 'we all run our nodes and take down the government', but we exchange as peers, like cash. And that's the whole point. It's electronic digital currency. Now all currency effectively goes to what is known as a token. And I think the first - at least the first one I know about that is a high level British case - is the case of mixed moneys, which is a 1605 case talking about physical tokens, which was tokenized sterling. So the British didn't want to actually send silver over to Ireland, so they gave these little nickel tokens to the Irish people and a really smart Irishman managed to arbitrage the difference because physical silver and nickel tokens were being done differently in different price because people didn't trust the nickel ones yet. And he arbitraged that made a whole lot of money off of a British lord who then got really upset and because of the actual law and everything like that, the clever little git of an Irishman basically won. So that was actually set in law, the whole nature of tokenized money going back that far. And what I've taken is this concept of what is a token for value in any sort of exchange of coins or anything like that that we have is really a token. So how do you make that? Well you have something that is an indivisible item, you can't cut a 10 Euro coin in half and have it valuable anymore. You can't cut a single Satoshi in half and have it valuable anymore. But you can have lots of them. So a Bitcoin is effectively 100 million of these little tiny tokens that are individually not worth much. But just like if you get a bag of gold dust, each grain of gold is worth a certain amount. By itself you're not going to get anything from it, but when you put them all together and you've got that big bag, then suddenly it's valuable and you can exchange. But like all these other things, tokens can also be used for other things. So I can sort of paint the back of that token and say now it is a special token that is actually worth more, not because it's a Bitcoin itself or whatever else, but because it is now a digital cinema ticket or it is a method for opening an

electronic door or all sorts of other things. So as a token, I can have it as the base level that pays miners. And this is why it's money, not because people are in a barter system like they are in exchanges. When they're doing that, they're not actually using bitcoin as money. It's money when you pay for goods and services. When I go to a miner and that node is paid to transact and process my transaction, the miner is accepting bitcoin as money. When I go to a shop and buy a coffee for bitcoin. It is money. But when I go to an exchange and I treat it as a commodity property item, then the Law Commission and others are correct, saying that this is just digital property and it's not money.

Ryan X. Charles [00:05:53] OK, so I have a follow up question, but I want to intermix my questions with the participants here. So does anybody have any specific questions you want to ask Craig? And if you can come up here, if you do that, we can speak directly into the microphone. Yeah, come up.

Questioner [00:06:13] Sometimes you talk about how when he created Bitcoin, IP to IP was one of your original visions. And now it sounds like we're kind of talking more about SPV and kind of stop talking about IP to IP. So are they the same? Cause they're both about sending directly between peers. Or what's the difference?

Craig Wright [00:06:35] So the original Bitcoin code didn't have SPV included, but IP to IP is really how you want SPV to work. So what you would have is a lightweight client that doesn't have the full node, doesn't keep all the blocks, just maintains block headers and its own information. So it scales a lot better because rather than having to have petabytes of information for every phone in the future, then all you need is the block information, because reality is that you don't need to or want to validate every single transaction on an earth. This Ethereum model where they're talking about everyone needs to validate that everyone is doing everything correctly, that doesn't scale. Your limit is you can only ever do what the smallest computer can do. So that's why Ethereum will have a problem. They can scale only up to the level of Raspberry Pi they want to sort of drop off the network. Now, in future, I see IP to IP and other things like near-field communication or even something like Bridgefly where you have distributed Bluetooth type networks. All of those would be a method for having SPV. So it'll be really difficult to stop Bitcoin in reality because I don't know if you know about Bridgefly or anything of this, but Bridgefly is one of the protocols that are used as an open Bluetooth system that was used in Hong Kong, for instance, for message sending around when they were having all the problems with the Chinese government and things. So they were shutting down the Internet. But what do you do? You just turn on Bridgefly and you hop between phones. And you end up with a wide distributed peer network and SPV could be built on something like that as well. So I said IP to IP, but I'd like to see Bridgefly. And I'd like to see all these other protocols as well. Imagine trying to stop if you're in a repressive government, not like Britain or something like that. You're an oppressive government and they want to stop Bitcoin. Well, now you can't. You're going to have to ban phones, ban all these other protocols, and you won't be able to even detect them. So getting your transaction out and spread would actually be simple. And it's important because the original protocol, the original way it worked with IP to IP wasn't just about sending the Bitcoin transaction. You had both online and offline so you could actually send messages between nodes. And when you're communicating and connecting to the other person, you could - it was rudimentary and ugly, I admit - but I could send a message. So if I was connecting to Ryan, I could give him a little message saying, 'yeah, I want to buy the the Money Button, widget number, whatever. And this is the colour I'd like it in. And if you make it green, it'll be better.' that sort of thing. And I could put that and he could send me a message back and go. 'We don't do green Money Buttons.' And then I could go, 'but I wanted green' and we could have a little conversation

before we even finish sending a Bitcoin. And none of that needed to go on chain. So we could actually have a combination thing. Or we could actually provably build it into the transaction by having hash puzzles and things to show we've got our communication log and we keep a hash of it so that we can prove if we need to later in court and things that we had that conversation and that we have done KYC if we needed to or we have done all this other stuff. But no one on chain will ever know. So we can privately maintain information as well as publicly exchanging. So does that give you an idea?

Ryan X. Charles [00:10:47] All right. I'm super tempted to ask follow up, but I want to make sure I don't ask questions when other people have questions. I mean anybody. Yeah, Joshua.

Questioner [00:10:53] My question is, do you see any concerns with encryptin g PII on chain?

Ryan X. Charles [00:11:02] Whereby PII, he means publicly identifiable information.

Craig Wright [00:11:08] Yes and no - depends on how you do it. There are always problems if you're sort of collecting lots of other people's data and not maintaining good integrity of things. So if you are a provider who is collecting lots of other people's data and managing it for them and you lose access, then again you get another Equifax, you get another Target, you get another whatever else. But on the other hand, if you're doing it in conjunction with the individual where they maintain their own security, then you could be attacked and then it could go through phishing and all that, but it's not as risky. If the individual gets attacked they can lose their own information and they could have multiple levels and different security layers and they could have keys on smart cards and all sorts of things like this. So if done right, it could actually be a very good idea. Now, people will say eventually all encryption gets cracked and that's true. ECDSA even if there's no security vulnerabilities, because you lose a bit of key length every 18 months - 15 to 18 months -, then eventually all of that's gonna be eaten away. And in a hundred and fifty to a hundred and seventy years from now, the current ECDSA implementation in Bitcoin is going to be broken and we'll have to have something else. Maybe ECDSA is version whatever which is 512 bits and that would give us more time. But the reality is, I don't really - I mean some people might - but I don't care if my personally identifiable information now is cracked in the year 2305 and people want to look up my life because it won't really bother me. I don't think.

Questioner [00:13:14] Thank you Craig. There's been a lot of conversation among us about how to manage voting. In the earlier conversation, you had mentioned that you'd been spending a lot of time on that. It occurs to me that there's probably a couple of main categories of this sort of thing. You have one like outline in the white paper where you have like a 'one CP one vote' type of a situation that's a little bit more oriented around skin in the game. And then the other type, which is more about like equal representation of a person, which is a different challenge. And we saw kind of a boom with the Internet trying to explore these ideas a little bit with things like Reddit where people could vote on things. But we've discovered how easy that is to game by creating a whole bunch of fake accounts and bots that can just make things appear to be more popular than they are. With the last Cambrian there was conversation after the CoinGeek conference where we first learned about R puzzles and there were some ideas floating around then about how you could craft a transaction such that a miner needed to do a certain amount of work in order to solve this puzzle. And this wasn't something where kind of the immediate Bitcoin solution that everybody thinks of is 'why don't we just make the votes cost money?' But

that doesn't really solve it because you can just create accounts and be paying yourself. And it really is no improvement. So I'm curious about how you see, you know, quantifying the value of information with voting with with with Bitcoin and how how we might do that going forward.

Craig Wright [00:14:56] This is a difficult question, because the reality is there's not one form of voting. Where people say voting, there are all sorts of things. There's representative democracies. There's full open democracy, there's all of the issues that come with voting systems. So how do you ensure that someone hasn't sold their vote? How do you ensure that someone isn't under duress being forced to vote a certain way? How do you allow that person to verify that their vote is correct and recorded, but not be able to show th at to another person, to show 'yes, I voted for you. Give me the money'. So the actual technical solution is generally a lot easier than the general real-world scenarios here. So there are lots of aspects to this. So if you're forming a company or something like that, then what you're doing is creating something that aligns to rules. In some ways that could be something like a proof of stake type model, which effectively shares are. If you own one share, you have one stake. So that would then allow you to create things like corporate models, et cetera, where different voting rights exist, mirroring existing legal systems. It becomes more difficult when you start doing things like voting in elections. So methodologies there would have to include things like an identity based issue against a blinded certificate. Now that all relies on seeing things like CLP or E- cash type ...they're more advanced than E-cash, we'll say E-cash type Shaumain models. Lots of people after Shaum invented way better versions of blinding. But what you then also need to do is something Microsoft extensively did in the early days, which is called traitor tracing. So if someone intentionally cheats or tries to double vote or sell their vote or anything like this, you need a way of exposing the individual. Yet if they haven't done anything wrong, making sure they're private. There are some areas that I'm working on at the moment doing all these things. So I know a little bit about it. But because I'm a nasty person who patents everything, I'm not going to actually tell you all the solutions we've got until they're ready.

Questioner [00:17:38] Just to follow up on that quickly. I mean, the part that I'm actually most interested in is, is the is the former where really we're trying to reinvent a system similar to Reddit, where we are valuing and expressing the value of information and we can kind of flip things to the top and such.

Craig Wright [00:17:53] So what you would also want to be able to do is have a pseudonymous identity linking, which you can do. So I've mentioned before that you can have additive keys, so you could actually have a registered identity key and a provable index model so that you could actually have a blinded secret that gets issued by the Reddit thing or something like this. Plus a chain of indexed values so that you have a new key every single time. That will then allow you to appear totally as if you're not that person at all. So you could even vote without leaving a record. But you also still have an audit trail that links you back to an original identity. And it could even link using a HMAC or something where you actually have the index value in the HMAC which is - simplest way to put it as 'a hash with a secret' like a password. But we have the indexed value so that we can say that maybe you have not been on the system for 20 years. Near the Reddit, I buy an account and I leave it sit there and doing nothing, but rather how active have I been? I don't know who voted, but I know this guy has voted a million times and has spent. And I can also tell that I haven't voted on my own system, that it is a real person who has voted on different things and potentially even get a run down without knowing who they are. So there are ways of doing that. What you are then doing is creating pseudonymous key

systems and identity that actually are separate to the the main Bitcoin protocol. And some of the things I've envisioned from when I said identity separate, I didn't mean you just lose identity. I mean you start creating systems to manage it privately.

Questioner [00:20:04] I think, like you said earlier in the SPV talk that Bitcoin doesn't get rid of middlemen. Can you talk about what it does do to middlemen? Does it make them compete? Have to be more efficient? Does it get rid of rent-seeking middlemen? Anything like that.

Craig Wright [00:20:18] Bitcoin doesn't get rid of the middlemen. It gets rid of trusted third parties. But it doesn't mean you can't build systems using Bitcoin that don't have middlemen. So that's that's where I should explain more. So because it's IP to IP, peer to peer and I don't need a trusted third party to validate between things, I can have a middleman if they're more effective. It's really an economic thing. If that middleman is cheaper and provides a good service, then I'll use them. Now one thing people don't realise, I used to do a lot of work for credit unions and what are the equivalent of savings and loans in the US, small banks and things like this. With the changes after the 80s and into the 90s, a lot of those basically got sucked up and eaten by big companies because they weren't able to do things like trusted third party services and the big banks really locked them out. This is one of my complaints about the changes of the banking system. It's not banking that is a problem. It's where the greed of a few people who are meant to be society's alphas have consumed what used to be there before, and those banks were still middlemen, but those banks used to actually get involved. They used to actually get to know the businesses that they were dealing with. They didn't sell the home loans to the highest bidders. They actually were involved making sure that people could pay their money on time. They worked with farmers to ensure that they could fund this year, next year and whatever else, because it wasn't 'how quickly can we make a small profit now to get my bonus'? It was 'how do I build my constituency of customers over 10, 20 years'? So what I'd like to see is people making effective third parties if they're third parties, ones that basically rather than me and you dealing with each other, this third party says, I can make your business better. I can actually come in here and help you grow. That's what a third party should be valuable for. And when I say alphas, I mean, we look at the big businessman making lots of money as the alpha. And I think that's an important concept for us because we are a tribal species. And the alpha is rewarded. And we generally don't mind as a tribal species until they don't do their job. And we have all this history where the alphas out there, we give them all these special benefits because they're going to die first. He's the guy when the big tiger comes into our village, he's gonna stand there with the spear and try and stab it as he gets ripped apart. That's what alphas do. And that's what we expect from these banking leaders and everything like that. They're getting 60 billion dollar bonuses because they're meant to fall on their own sword when things go wrong. But they're not. Basically, they go, 'oh, well, stiff shit. I know you lost your home. I'm going to retire. Damn - need a 100 million dollar bonus. And then I'll leave because I'm so generous. I'm quitting'. And that's what people are really aggregated ...It's not the banks that are the problem. It's these parasitic so-called top level alphas who are trying to consume society. And we need to get back to this scenario where people who are bankers and and middlemen and whatever rules are actually giving to society.

Ryan X. Charles [00:24:27] So this is kind of an interesting thing, because when I talk with you, I think you have a huge amount of knowledge about all this stuff. And I think you have a very realistic perspective. But what you just said sounds kind of terrifying to some people. People are like, for instance, I'll talk with people that are - I hate to use these words and stuff like this because it's so polarizing - but I talk with a lot of people actually

that identify as things like communist, socialist, Marxist and things like this that would be really sort of repulsed by some of the things you just said. Can you comment on that? I mean, like, you know, in terms of, you know ...I'll ask it this way. Do you have an ideology in what you just said or is this based on, like, you know, facts about the world?

Craig Wright [00:25:14] I'm one of these horrible people who change my opinion as people give me new evidence. So am I a particular ideology? Well, I'm a Christian, but other than that, not really. I look at new evidence. I look at new things. I read lots of different parties and I update my views accordingly. So if someone proved to me that communism could work and they actually proved it, I would listen to them. Except I don't like the outcome. I don't like this idea that we all live in little wood houses and cabins and things like that. Like Marx envisioned or the Ghandian idea that we're all self-sufficient. And I lockm my wife at home spinning yarn until the wee hours because, well, that's just what you do. So I don't actually think even if you could scientifically prove it. I would like it because I think they're bad ideas. But ideology, I think growth is important. But that's not just making money. That's where people go wrong. So a lot of the concept that we've got in the last 10, fifteen years about what makes success seems to be this idea that I've made money quickly. My ideology is anti-fraud and corruption. And I think a lot of these people sit there with this false idea of what is libertarian right now need to understand that libertarian requires someone actually enforcing fraud. You can't have a mob of people running around and then lynching everyone you think did something wrong. You have to have courts. You have to have a justice system. Criminals are incentivized. People are incentivized. If you know you're going to be caught then you do less crime. If you think you'll get away with it, you do more.

Ryan X. Charles [00:27:20] I think that, you know, for someone that does identify as communist and I say this only because it's so sort of intrinsically like a lot of people really believe this type of thing. When I see what you're saying, I detect in you a strong scientist because this is very scientific of you to to change your mind when you have new evidence and stuff like this. Do you see anything at all about what people believe if they if they're communists that you actually agree with?

Craig Wright [00:27:48] Not really, I don't like the whole class thing and bourgeois versus the worker or anything like that. I think that's designed to cause dissension. So what I will say about the communism bit is it seems to be designed to cause problems intentionally, which is really a way of enabling people to have power grabs. So someone will always rise and take over. If you look at sort of the cycles that Plato talked about, you have democracy goes into a demagoguery and and sort of goes into mob rule and then a tyrant will come and etc., etc. and it goes through these cycles. And that was why the Americans tried to create a republic, because you wanted to balance the executive. The sovereign, the president with the aristocracy, the Senate and the people, the mob, as they'd call them, the general, every populace. And you don't want to have any one of those aspects too powerful.

Ryan X. Charles [00:29:04] All right. I have one final question for you that's a bit of a sort of thematic question, given that we're at Cambrian and we have a lot of developers and entrepreneurs and people that are trying to build the future of Bitcoin. For those of us that are either working on a project or a business or something like this, would you have any advice like what do you think we should keep in mind as we go about building the stuff that we're building? What what should we be doing next?

Craig Wright [00:29:25] I think you should find things that people actually need solved - market niches and things like this and ignore the Silicon Valley idea of you just raise money. What you really need to do is find a way of making something profitable. I mean, if you look at all these things, they're starting to fall apart. Uber is already starting to show itself as a basket case because it was, WeWork is a total scam and a basket case. I mean, 'we're a technology company because we put sensors on the doors'. I mean, really? And then Silicon Valley venture capitalists go, 'wow, big data, because every time someone opens the door, we can record it. Yay'. And if you start thinking about some of this, it's problems that are being created so that they can raise money. And what you should be doing is problems that are real problems and the world is full of them. I mean, this world is full of problems that need solutions. We have an infinite amount of things that people would love to do if you don't believe that. I have an infinite amount of things that I would happily have people doing. I just don't have the resources to have an infinite number of people working for me. But the reality is there are so many different problems, ones that people don't even think about. It's the old Henry Ford bit. Why didn't he sort of make a better horse and carriage? Because, well, like customers would ask him for because well, too bad there's another problem. I've seen it. I'm fixing this one. And it's really what they wanted fixed. So find a real problem, find something that is. And I name things all the time because I see things that are problems that I either face or know people who face or whatever else. But in everyone's life you'll go through just walking about interacting with people, being in business and you'll notice things that are frustrating, things that could be done better. And you'll you'll think sometimes, 'oh, if someone automated this or if someone integrated this in a better way or if the records were kept better, or if we could have an exchange that allowed me to not have to verify people so much or. Dot, dot, dot, then you can start thinking of a business around that. And if it's something that lots of people have that problem, then you're gonna make money.

Ryan X. Charles [00:32:08] All right. Well, thank you very much, Craig. This is awesome to talk with you, as usual. There's always lots of information, a lot for us to process. So thanks for coming at the event and we really appreciate your time.