

Transcript

Blockchain Chess Analogy interview

David Bradley Talks to William Ralston-Saul

David Bradley 00:01

William Ralston Saul gives this fantastic description of blockchain. It's clear, it's concise. And if you don't understand blockchain, you soon will listen to this. Here goes,

William Ralston-Saul 00:13

Well, first, I'll explain it the way it was explained to me, which which caused me not to understand it. So the typical thing is if somebody says, well, what's a blockchain and it happens to be somebody in the room who understands? They'll typically say, Well, it's a trustless, decentralised, permissionless ledger. And it's amazing. And when somebody first said that, to me, that meant precisely nothing. It actually meant so little to me that I decided not to ask anybody else for another six months in case they might just give me the same confusing answer. So, eventually, one day when I actually did manage to get my head around it, I realised that yes, a trustless permissionless. decentralised ledger is an accurate description. But it but but it's not the best way of explaining it. So what I'll try and do I know that you already understand what a blockchain is, but I will for the sake of the listeners, I will explain it to you

David Bradley 01:12

Assume I know know nothing.

William Ralston-Saul 01:14

I'll assume you know nothing.

David Bradley 01:15

A little bit of knowledge is a dangerous thing.

William Ralston-Saul 01:17

It can be it can be. And we all learned something all the time. And particularly with the blockchain world. I mean, it moves so fast. But I think a good way to start is actually to explain the power of decentralisation and how that can protect people and transactions. So if we do you David you play poker or chess,

David Bradley 01:39

I play chess and I play poker occasionally.

William Ralston-Saul 01:42

Okay. All right. Well, let's, let's imagine that one evening, after dinner, you and I sit across the table, and we played a game of chess together. And as they often do, in chess games, every move is written down. But in this case, we're playing for money. We're playing for £100. And so every time I make a move, it's in the book in one book, one centralised Ledger in the middle of the table. Okay, one, we call it the centralised ledger, but essentially, it's just a book with the records in it. And every time you make a move that goes in the book. Every time we bet that goes in the book. Everything that happens for that entire game gets written in that book,

David Bradley 02:21

Like a ledger. It's like a ledger.

William Ralston-Saul 02:22

It's like a ledger. It's exactly what it is. Yeah. So at the end of the at the end of the game, I beat you, I take 100 pounds of you and you go to bed extraordinarily upset with mortified and lying in bed. You're thinking, God, I hate William. Somehow. He has, he's cheated me.

David Bradley 02:43

He's cheated me out of £100.

William Ralston-Saul 02:46

Exactly. And God. And I just, I don't know how, but somehow I got to get my money back. Well, it's lying in bed, stewing and your misery, you've got two options. One option is the next day at breakfast. You can say, William, I'm not happy about the result last night, I want to I challenge the results. And I want to get the ledger that let's say it's sitting in the book, but I want to get it out. And I want to replay the game in accordance with the ledger. And I'm sure if we replay it, so there was something in there where you cheated, and I'll get my 100 pounds back. Okay, so That's option number one. It could work. Probably. That's option number one, option number two. And this is a far more effective option is for you just to sneak downstairs in the middle of the night. Find the ledger, get it out of the cupboard, rub out a few few details, rewrite the ledger, then the next morning, challenge me to the game according to the ledger. And hey, presto, you got your 100 pounds. Okay?

David Bradley 03:50

Yup, bingo,

William Ralston-Saul 03:51

So that that ledger or that book that represent a centralised system. It's it's a system whereby you, on your own managed to go downstairs and change history. And as a result, defraud me out of my hard £100.

David Bradley 04:08

I wouldn't do anything like that.

William Ralston-Saul 04:11

So unimaginable. That's why this is a purely hypothetical, hypothetical conversation. So, So So that's option one. So anyway, the next day, you want to rematch and you say, and because we are arguably the greatest chess players, since the beginning of mankind, we decided that we're going to do our rematch in the middle of Wembley Stadium. And when we sit in the middle of Wembley Stadium, we're also going to invite 80,000 spectators and the spectators happened to be the most professional bookkeepers from all around the UK that have come to watch our game. Okay. And as we play our game, we don't write down anything but they write down every move every bet, X, Y and Z as they're watching our game as we're in the middle of Wembley Stadium. And once again, I win £100 pounds off you. This time you go to bed and you're like 10 times more upset than you were the night before. And you lie in bed stewing in your misery and you've got the same two options. How am I going to turn over the result? Well, is this the same thing applies, but this time is a bit more complicated. You can challenge me the next morning to replay the game. And assuming we have infinite amount of time, we can invite back all the bookkeepers. And we can replay the game 80,000 times in accordance with the 80,000 records that we have. And if you can get 41,000 those records to go in your favour, then you could turn over the result. I would say that that's so unlikely that I would say it's it's it's as close to impossible as it needs to be. Okay. So that that's difficult. The other option is to hire an enormous team of cat burglars to somehow miraculously track down all these bookkeepers. Find their Ledger's, change all the results, and then and then invite them back for us to replay the games. And that's also impossible, because you don't know where the bookkeepers live, you don't know where they keep the ledgers and you couldn't pull something like that off in that period of time. Okay, so So by inviting an enormous audience to witness what we've done, you have created a permanent record in history that cannot be tampered with. And although it sounds a very simple thing to create a permanent record in history that cannot be tampered with. It's actually not that simple without a blockchain. And that's what and that's what a blockchain does. It's a multiple records hold in multiple places to make something a permanent record. In the case of a blockchain, it's not 80,000, bookkeepers, it might be 80,000 computers. And the computers might be in every country in the world. But they all keep a record of what's happened. And because they've done that, you don't need anybody else. You don't need a bank to tell you that you did this or that. It's all just recorded everywhere. Okay, the only thing you need is transparency, you always need to be able to access their books, so you can see what's inside it. And a blockchain also allows you to do that.

David Bradley 07:04

Okay, well, I think that's one of the most fantastic descriptions of how it works. I mean, brilliant, except using computers, how does the transaction get recorded so that it can't be in any way technically, or physically tampered with?

William Ralston-Saul 07:22

Yeah, so so the way that the way it really works, and I can continue with the analogy is, let's say we're still sitting in the middle of Wembley Stadium. And, and if we finished our game, you're upset, but I decided to improve your mood that I'm going to transfer one bitcoin from my wallet to your wallet. Okay. All I really need to do is I need to stand up in the middle of the stadium and shout out "everybody, I want to send one bitcoin to David". And 80,000, people are going to hear me say that, right. Now, the only question is from those 80,000 people who's the first person that gets the write down the record before before they share it with everybody else? Okay, and that's this is where we come on to Bitcoin

mining. Bitcoin mining is a competition to be the first person to write the new block of information. So we're basically yeah, in the middle of the stadium, I can I can, I can call out that I want to transfer one bitcoin to you I broadcast the information. Yeah, that I want to do. And that's exactly how it works with the blockchain from your wallet, inside your computer, you broadcast to the blockchain, that you want to do that you want to send a Bitcoin. And that and that is is sent out. And, and it's picked up by the the validator community, and

David Bradley 08:50

sent out over the internet to the various computers that have a copy of the blockchain.

William Ralston-Saul 08:56

Exactly. And they can either choose to add it into the next block or not. So if you pay a high enough transaction fee, you will essentially get a place in the next block. So there's, in the case of Bitcoin, 3000 transactions approximately can fit into each block, and there's one block every 10 minutes. Okay, but the question is, if we come back to our stadium analogy, is if I stand there in the middle of stadium and shout out, "I want to transfer one bitcoin to David", and they're all ready to write it down in their books, who gets to write it down first. And that's the competition. That's the mining Bitcoin mining competition is this competition to see who can who can write it down first. And very simply, I could also stand there and say, oh, and I'm thinking I'm thinking of a number in my head between one and 1 trillion. And the first person to guess it gets the right gets the write down the transaction first. And they'll all shout out their numbers, and somebody will guess it right. And I'm like, okay, so it's you, you get to write it down. And that's, that's a real simplification of how Bitcoin mining works all these these these mining farms around the world. They are essentially trying to trying to guess what the answer is to each block. And when one of them guesses it right? They win the block, they get a reward for doing it, which is 6.25 Bitcoin and they print the block and then share it.

David Bradley 10:19

William will be speaking at the next Revellers' Club event which is "Understanding the Opportunities of Crypto" it is going to be held in Battersea at 6:30pm on the 23rd of February. All the details are at www.revellersclub.com/crypto-opportunity that's www.revellersclub.com/crypto-opportunity. Hopefully see you there.