What Is Decentralized Finance?

https://mindmatters.ai/podcast/ep202

Robert J. Marks:

Greetings welcome to Mind Matters News, I'm your cryptic host, Robert J. Marks. We continue our chat with Adam Goad and Austin Egbert about Web3 and the future of the internet, things like decentralized computing, blockchain, and how things are going to happen in the future. And having looked at this, man there's a lot happening. We're going to talk today about decentralized finance and here's what I understand. And we're going to let Adam and Austin fill in the details here. When you pay Uber for a ride, or anybody else, you use a bank or a third party like PayPal, or Visa, or MasterCard, or something like that. Decentralized banking, hopefully, will let you pay for the Uber driver directly without a third party. And again, this can be done using decentralized finance. So Adam, what is centralized finance? What is decentralized finance, and why should I care?

Adam Goad:

Good question. So centralized finance is the system we have now. It's like you described whenever you want to pay for something, you would take out your credit card, you would swipe it and it would go over the internet. It would tell your bank that you want to pay. Then the bank would figure out who you're trying to pay and send them some money, if you can. The currency is also regulated by the government we have in the US. We have the federal reserve bank and they have all sorts of control from how much money is printed, setting interest rates, all sorts of things. With decentralized finance, you do not have these central authorities having this power over the currency. So like you said, if you want to pay that taxi driver, you could just send them a transaction directly using Bitcoin, or Ethereum, or something. And then those currencies cannot be blocked and not run through a centralized exchange of any kind. They can be sent just through the distributed system of the blockchain that we talked about previously.

Adam Goad:

And the record would be in the public ledger, you sent him money, he could confirm that, and you can both go along your way. So this has several benefits. It prevents any kind of centralized regulation. So you can have regulation in a decentralized finance. Last time we spoke briefly about DAOs, decentralized autonomous organizations. Several of these larger DeFi, decentralized finance projects, are run as DAOs, where people who have invested money into them, do get a say in how it is run. And it is run purely as code. So anyone can confirm this code and what it's doing, and that it's doing what it says it's doing. And people can make proposals and vote on changes to this code. And the code can only be changed if everyone approves these changes, or at least a majority, or whatever the rules are for that particular DAO of how many people must approve.

Robert J. Marks:

So the bottom line is that individual users have more control and transparency over their finances. I like that. You don't have to go through a third party. How does this work? How do the blockchains enter into this? I'm sure that the blockchains enter into this in order to establish trust and stability, in terms of the decentralized finance, what's the role of blockchain here?

Adam Goad:

Right. So you mentioned trust, the blockchain adds trust because it is a trustless system. It does not require you to trust anyone in order to use it.

Robert J. Marks:

Okay. This is interesting, because I've seen the word trustless and trustless doesn't sound good, but in the contexts of crypto, it means you don't have to trust any human. So trustless always refers to humans. Is that right?

Adam Goad:

That is my understanding of it. I haven't looked at a dictionary definition, but that's how I've always interpreted it. So, if you want to transact on a blockchain, then in order to use any funds that are in an account on this blockchain, you'd have to have the private cryptographic key for that account. That's going to be a long string of letters and numbers that you should keep private, because anyone who has that string can have complete control over the funds in that account. So using that private key, along with your public key, which in most cases is your address that people would use, or a derivative of it. Then you can encrypt any transaction you want to send into the blockchain, send it off to the blockchain. And it's encrypted in such a way that it can be confirmed, that it was signed by your private key. As long as someone knows the public key and the public key can also be derived from the way it was signed.

Adam Goad:

So then, after the blockchain and anyone else who wants to is able to confirm that I sent this transaction to the chain, the ledger, the chain itself, would then have a record that my account sent the money to your account. And you can go check the chain. You can use various services that will check it for you and just tell you your balance. And you'll know that I have sent you the money and there it is. We didn't have to talk to any banks. We could've used any number of Ethereum nodes, or any other kind of chains, nodes distributed all over the world without a centralized authority having a say in things.

Robert J. Marks:

Interesting. It does seem though, like blockchain has replaced the bank is the third party. So what's the difference here? Is that it that the blockchain doesn't tell anybody what's going on, or what's the advantage of using blockchain instead of a bank?

Adam Goad:

So, it's not that blockchain doesn't tell anyone what's going on, instead it tells everyone what's going on.

Robert J. Marks:

Okay. So blockchain knows how much you paid the Uber driver?

Adam Goad:

Yes. And everyone else in the world can know too. But what they don't know is who you are, or who you paid or, why.

Robert J. Marks:

Oh, now that's interesting. If they don't know who I am, who I paid, or why I paid them, then that looks like a lot of privacy. So that's the advantage that this decentralized finance gives to you, is that right?

Adam Goad:

Exactly. All that's recorded is that this address paid this address this much at this time. Who owns those addresses, why did they feel the need to send that money? None of that is stored. And you'd have to know a lot about someone to figure it out.

Robert J. Marks:

Isn't that interesting, okay. Where do these decentralized finance blockchains live? Do they live on your computer?

Adam Goad:

So the blockchain itself lives on anyone's computer that wants to have a copy pretty much. It can be fairly intensive to have it. So you need a pretty powerful computer. If you want to be what's known as a node. So a node is a computer that stores a copy of the blockchain and helps to process the blockchain. As new transactions come in, you can also set up a miner to be on a node, to try to mine new transactions. And basically then if someone wants to send a transaction, they send that transaction to a node. And then that node will work to send it through the network, to get it to the miners, to get it put onto the chain.

Robert J. Marks:

I see. So it's just like everybody has copies of the blockchain, but nobody knows what's inside of the individual links on the chain, if you will. Is that right?

Adam Goad:

Nope. Everyone knows what's inside every link.

Robert J. Marks:

Oh, they do know what's inside every link, but they don't know who it is, or why you paid it. Okay.

Adam Goad:

Right. There's a website you can go to. It's called Etherscan, etherscan.io. It is one of the most popular websites. You can use it to browse any transaction you want on the Ethereum blockchain. You can search them by who sent them, who received them, when they were sent all sorts of things. And you can look at every single transaction ever sent if you wanted.

Robert J. Marks:

Oh my goodness. Okay. Well, I bet you, the IRS is happy about that, aren't they? By the way, if you know that person A was a transaction on one of the chains of the blockchain, do you know that person A was also a participant in blockchain 36?

Adam Goad:

Yes. So, well on a single chain, yes. You can say, "Okay. If I know that this person sent this transaction, then I now know the Ethereum address," whichever chain it is. And you can look at all the other activity

for that address. And you can see where it sent money. You can see who those people sent money to. It's all there.

Robert J. Marks:

Isn't that interesting.

Austin Egbert:

But on a separate blockchain, that address isn't the same as the address they might have on a different blockchain?

Adam Goad:

Correct. So in order to figure that out, you would have to see them try to send the funds through to the other blockchain using various services, or you would have to, if they did it through a centralized cryptocurrency exchange, you could have the exchange. You could force them to report to you what addresses they sent to and such, because the way the centralized exchanges work such as Coinbase, they are a subject to government regulation. So when you sign up for an account on one of them, if you're going to be transacting at a certain amount, some of them, I think there is a small amount you can do without having to do this. But if you get to a certain level, you are acquired to complete what is known as know your customer, KYC. And that's a process, where you have to go through and prove your actual identity to the exchange. You have to send them a copy of your driver's license, or something like that, so that they can then tell the government who you are and file your taxes accordingly.

Robert J. Marks:

But this is only for certain blockchains, is that right?

Adam Goad:

This is anytime you want to use a centralized exchange. So the centralized exchanges are by far the easiest way to get money in and out of cryptocurrency. So they will let you hook up to your bank account, or hook up to your credit card, and put your us dollars into cryptocurrency through their service.

Robert J. Marks:

I don't know if you remember, but the FBI at one time was monitoring telephone calls and they didn't monitor who called who, but they did say A called B, A called C, C called D, and then B called D. And so they built up this tree of interconnections and they maintained that they were not violating anybody's privacy, because names and telephone numbers weren't associated with that. But they build up this great tree with lots of clusters and they could, if they found out one node, like if they found out the identity of A, all of sudden, the other ones begin to fall down with certain probability, with that knowledge. The blockchain, as you've described, it kind of reminds me of that. Is there any truth in my analogy?

Adam Goad:

Yes, you have it exactly right. If the FBI, or any other law enforcement agency is trying to track down some kind of criminal who's using cryptocurrency, they most likely know what transactions they're trying to follow. They just don't know who is on the other end of those private addresses. So as soon as

they figure out who owns one of them, it's the same thing. They can try to guess who owns these other ones based off when they were paid and how much they were paid and how often, such like that, exact same sort of thing.

Robert J. Marks:

Interesting. I listen to the book, American Kingpin, and it was about a guy that called himself, the Dread Pirate Roberts, who ran a website through tor, which is a very private internet service, and they sold drugs. And the government, I think, through the DEA, went through and tracked all of the finances, because one of the people in the DEA bought some drugs from this guy and he knew where it went. And there all of a sudden he was able to determine all of the other places that this money came from. And they determined who it was, but they didn't find the identity after some, oh, what do they call it? Leather shoe investigation, where they had to go out and use normal intelligence in order to do it. It's just a fascinating book. If anybody is looking for a good read, or a good listen, American Kingpin is just riveting.

Robert J. Marks:

So that's the way that they eventually found him is through this process that we're talking about just like the FBI tallying all of these telephone calls, but not saying what the number was, and not saying the identity of the person, but simply connecting a bunch of nodes about A calling B, and B calling C and then C calling A, et cetera. That's really interesting.

Robert J. Marks:

One of the things I read, and looking at this for the prep today, because I understand very little about blockchain and I really appreciate your time and your effort to explain it to us. But somebody said that blockchain hackers stole nearly $1.3 billion with 79 hack events, through the first quarter of 2022. What's a quarter, three months? And so in three months they were able to still $1.3 billion reading deeper, though, it seems that the blockchain hackers took advantage of flaws in the project code, which I guess maybe in some ways was made public. That seems to be strange to make the code in a blockchain public. So it seems to me that if you're going to do this, if you're going to do distributed banking, you got to choose who you're dealing with very carefully, because some of the new kids on the block, aren't going to have the security that the older guys have. So who are some of the older guys, who are good people with lots of experience in distributed finance?

Adam Goad:

Well, to comment on that theft first a bit, I'm of course not familiar with every case, but a lot of times when people have the cryptocurrency stolen, it is because they fell for some kind of scam.

Robert J. Marks:

They were kind of phished in a way?

Adam Goad:

Yes, exactly. They personally gave out the secure key to someone, or they downloaded something onto their computer that was able to then trick them into doing something, or they submitted a transaction to something that was not what they thought it was.

Robert J. Marks:

I see.

Adam Goad:

And so I think a lot of also what you might have found are things known as rug pools. So that is where someone sets up a project, whether it be an NFT, or a new coin, or a decentralized finance system. And they tell everyone it's the newest bestest thing. And they convince all these people to invest in it. But really all they're going to do is take all the money everyone puts in and run away and it's not going to ever do anything.

Robert J. Marks:

I see. I like to pride myself in the fact I'm very hard to phish, but I have a bunch of websites and I ran them on a host called Bluehost. And I got this email from Bluehost one time. And it says, "You have too many files on the host server. You need to remove some. Click here to log in." So I clicked there, it took me to the Bluehost page. I entered my name, I entered my password. Then I hit return and nothing happened. I was phished. What they had done is they had taken an exact duplicate of the Bluehost site and they had replicated it. And by doing with this email and me trying to log in, I was phished.

Robert J. Marks:

The next day all of my files had viruses in and I had to contact somebody to scrub all my files and I moved them off of Bluehost onto another server. And you think that you're immune to phishing. But man, I fell into that so easily. I guess I have to be less naive in the future. And that's what I've heard is that encrypting is something that is very difficult to break. And the only way that you can actually break it is through the weakness of the human element.

Adam Goad:

I have not heard of any case where a cryptocurrency of any kind was hacked by breaking the encryption. I've only heard of cases where it was a human error that caused the flaw or something.

Robert J. Marks:

I see. Okay. Now in talking before we started this recording, you mentioned something which blew my mind and that was something called flash loans. Could you talk about flash loans for a second and try to explain it to me so that I understand, as best as possible. These flash loans seemed incredible. What's a flash loan?

Adam Goad:

So a flash loan is a loan that you take out for a very short amount of time, usually a few seconds.

Robert J. Marks:

A few seconds.

Adam Goad:

But it can be for a very large amounts, like millions of dollars. So if you want to feel like a millionaire for a few seconds, you can go take out a flash loan. But the point of them, most often, is to use them for arbitrage.

Robert J. Marks:

Oh, okay. Well, first of all, explain arbitrage. I think most people know what it is, but I think we should probably explain arbitrage real quickly.

Adam Goad:

Yes. So arbitrage is when you see an opportunity to buy and sell something at a different price in different places. So let's say if you are on Coinbase and you can buy Ethereum for $2,000, but if you look at another cryptocurrency exchange such as Kraken and you see that over there, you could sell Ethereum for $2,100. You would immediately want to buy all of the cryptocurrency you can from Coinbase and sell it to Kraken. And you'd make a hundred dollars per Ethereum that you did in this manner.

Robert J. Marks:

Because there's this price disparity.

Adam Goad:

Yes, exactly. And by doing so you would equalize the price disparity between the two, as they adapt to the market.

Robert J. Marks:

Wow. 10 million for 10 seconds. Clearly, you pay a premium for this. You pay some sort of interest to borrow that $10 million. Is that right?

Adam Goad:

Yes. You would pay a fee and flash loans are often enforced through smart contract. So you would actually put these transactions you're going to do in the arbitrage, into the smart contract, so that the lender can see this and be satisfied that they're going to have the money back in 10 seconds. And you're not just going to run away with it. The transactions of them sending you the money, you buying and selling to do the arbitrage, and then the money being returned to them with the interest. And then the money being returned to you with your profits is all set into code that the blockchain executes and in that way it is trustless. And therefore you can trust each other.

Robert J. Marks:

Now to do this 10 million loan, do you need collateral?

Adam Goad:

So with the flash loans, since it is enforced through the smart contract, there's no need for the collateral. It is the risk of you and the lender that it's going to go well. And you both know that neither of you can run off with anything, because you can both trust the code in the smart contract.

Robert J. Marks:

Okay. Thinking about that though, if you want to do arbitrage between two different markets, for example, and you borrow the $10 million and the markets go kablooey, maybe the prices even out or something, I guess the only loss you have is the fee that you paid for the $10 million. So you risk that in a way don't you?

Adam Goad:

Yes. The lender would be risking that as well. They would risk that perhaps the value of it went below $10 million in those 10 seconds that you had it. So yes, there is risk involved on both parties there that it could not work.

Robert J. Marks:

I have heard that most computer trading is arbitrage. And in fact, there's some trading institutions that want to get faster cable so that they can do arbitrage more quickly than somebody else. Have you ever heard of that scenario, of these trading houses wanting to do arbitrage by beating the other person with the speed of their computers?

Adam Goad:

Oh yes, certainly. Cryptocurrency is a constant 24/7 market, where milliseconds matter. When you find these arbitrage opportunities, since there are so many people looking for them, it's constantly going. So it's very rare to find a very large one. So you are only going to find maybe perhaps a 1% difference between prices. And if you know that price is greater than the fees, you're going to have to pay to conduct these transactions, then you of course want to do your arbitrage. But like you said, at the same time you found that there's going to be dozens of other people who found that same opportunity, because their computers were also looking for it. So who gets there first? This is actually something I've been working on with an NFT project I work for. Then we've created, we call it the Hypernode. What we've done is we've taken very fast computer servers and we've put Ethereum nodes onto them. And we have also, I suppose, I have modified these nodes so that only select individuals can use them, in this case, the holders of the NFTs from the project.

Robert J. Marks:

Let's back up a little bit and define some of these things. What's a Hypernode?

Adam Goad:

That is the name we've given to the service we provide of these very fast Ethereum nodes that we allow holders to have access to. And we limit the access to only being available to the holders. So then that encourages people to, well, of course, enter into the project, but also, it provides insurance that our node will remain fast. There are plenty of public nodes on the Ethereum network that anyone can do. And if you download any kind of app to transact with Ethereum, it will have some kind of default node it applies you to. But by restricting who can use our node and making sure that we have very fast hardware supporting it and internet connection, we can provide our users with a faster connection to the blockchain than anyone just using a public node.

Robert J. Marks:

I see. And is that enough to beat some of these different trading houses? I have heard for example, that there have been trading houses that have geographically moved closer to the New York Stock Exchange and laid fiber in order to get in order to get quicker responses. That seems to be very difficult to beat.

Adam Goad:

So since the New York Stock Exchange is a centralized system, you have to be close to it in order to get those speeds. With Ethereum and other cryptocurrencies being decentralized, you can place a node anywhere and get that fast access to the network.

Robert J. Marks:

I see. So your business is for decentralized finance. So you don't have to go to the places like the Chicago Mercantile, or the New York Stock Exchange, right?

Adam Goad:

Exactly. There is no central Ethereum market in a physical location anywhere that you need to be close to. What matters is how close you are to a node and how fast that node is.

Robert J. Marks:

I see. So let me ask you, how close are you to market? Are you geared up yet? Are you selling these services?

Adam Goad:

Yes. We have been online for several months now.

Robert J. Marks:

Okay. With the stipulation that Mind Matters News is not being paid at all for this endorsement, tell me how somebody can find out more about your business.

Adam Goad:

The project name is Just Cubes and you can find out more @justcubes.io. J-U-S-T-C-U-B-E-S.io.

Robert J. Marks:

Okay. Well, great. Well, best of luck in that, I hope you become a very wealthy person because of that. One final thing that I'd like to ask you about is something called stablecoins, which you're going to have to explain to me. It turns out that most cryptocurrencies are incredibly volatile. They will go up and down, their variants, their volatility is just wild. Yet these so-called stablecoins are cryptocurrencies as I understand them that don't display this volatility, what's going on there. How do you do that?

Adam Goad:

So, yes, like you said, the crypto market can be incredibly volatile. Recently, the Ethereum market dropped 10% in a day. It's had wild swings in the past as well. But yes, stablecoins. There's a handful of these. USD coin, standing for US dollar coin, DAO, Tether. There's several of them. But what they do is they have something backing them. And by being backed by this, they are pegged to a currency such as the US dollar, there's ones for the pound, the euro and other such currencies around the world.

Adam Goad:

So the one I'm most familiar with USD coin, what they do is they actually go and they take a dollar bill and they put it into a bank vault for every single one of their coins that they issue. And you can go to them and you can say, "Here's five USD coins, give me $5," and they can do that for you. So since there is something actually backing and pegging this currency to the US dollar, it will always have value of $1.

Now there is a slight bit of fluctuation around it, just based off the momentary demand for it. But that usually is in the tens of thousands, or hundreds of thousands of as cent range of how much it changes.

Robert J. Marks:

Now, clearly in order to back up this USD coin, that's going to cost big bucks. Who fronts that big bucks and whoever fronts, the big bucks has to have a reason to do it, they need to get paid. So how does that work?

Adam Goad:

So there have been plenty of investors getting involved in different Web3 and cryptocurrency projects over the past few years. And they would get paid the same way that people who get paid for mining and such with, they would take a percentage of the fees that are provided to transact on the network.

Robert J. Marks:

I see. Okay. So every time you trade a USD coin, you are charged a little bit, almost like charging something on Visa, the merchant that you charge it to has to eat a little bit of the purchase price, because that goes to Visa, or MasterCard, or something like that. Is that a good analogy?

Adam Goad:

Yes. But in the case of cryptocurrencies, it is the one initiating the transaction who has to fund the cost of the fees.

Robert J. Marks:

Very interesting. I think that this decentralized finance is going to be a big deal. I was talking to an employee of a bank who said that banks really hate decentralized financing, or decentralized finance in general. Do you think that maybe banks are going to come and try to crush this decentralized banking, or do you think that they're going to go with a way of the brick and mortar stores, some of which have just gone belly up?

Adam Goad:

Well, like you said on one of our last episodes, "Always hate to make predictions, especially about the future." But I am certain that there are aspects of this I'm sure banks don't like, because it is taking away some of the palette. It's allowing people to borrow money, to do loans, to invest without having to go through the centralized systems, and therefore they're not getting a cut. Which one will win out in the end? I don't know. But I do think that this will be around for a while.

Robert J. Marks:

Yeah. It really seems to be exciting stuff and just an incredible thing for the future. And a thing to keep your eye on. So Adam, welcome. We've been talking to Adam Goad and Austin Egbert about decentralized banking and some of the things which are going on, which are pretty exciting using blockchain, which will allow you greater access and greater privacy in your financial transactions. So thank you again, Adam, until next time, be of good cheer.

Announcer:

This has been Mind Matters News with your host, Robert J. Marks. Explore more @mindmatters.ai, that's mindmatters.ai. Mind Matters News is directed and edited by Austin Egbert. The opinions expressed on this program are solely those of the speakers.