DeFi, NFTs, and crypto in business

Professor Raghavendra Rau

23rd January 2023

Introduction

In this lecture, I want to build on my second lecture “Love, Trust, and Crypto” to talk about DeFi, NFTs stablecoins, and other curious crypto animals in business.

What do you mean when you say you own something? For a financial asset, the answer is easy. For financial assets, ownership usually means an entry in some kind of database or the other. So for example, if you own a share, that ownership will be recorded in some kind of central depository institution. If you deposit money in a bank, the bank’s databases keep track of that money. So ownership of a financial asset is pretty much a database entry.

However, that's not true of a physical asset. What do you mean when you say I own a physical asset? Well, you might say that ownership rights are temporary; if someone stronger comes around, they can beat me up and take my asset away. You can use something as long as someone stronger than you doesn't take it away from you.

But in countries with a more developed rule of law, like the UK or the US, there is a different concept of ownership and that is about social norms. For example, you might think, okay, if I own the key to a house, that means I have the right to live in the house, but that's not true. Our neighbors know who lives in the house when you leave the house in the morning or when you come back in the evening. You have a right to be in that house. But if a stranger opens the door to your house using a key and walks in, your neighbours would not necessarily say, hey, that guy has the key, so he has the right to be in the house. They will probably call the police saying it's a burglar. So that's a social norm built around that concept of ownership. People agree that you own something.

But in addition to that, if you want to formally establish your rights among people who don't know you, there is a rule of law. And that rule of law exists on databases. For example, your ownership of a house is recorded in your title deed held by a title corporation and lots of other places.

But who maintains those databases? One possibility is the central authority, the government. For example, in England, back to just after 1066 when William the Conqueror invaded the UK, he instituted the Domesday Book which is record of who owns what and when. The Domesday Book is a series of database entries saying who owns which house and what other property.

Today, your databases are more likely to be maintained by intermediaries, such as exchanges, banks, and other depository institutions. But trust in these is fragile. For example, you could be expropriated by the government. It might decide to just take your stuff away for the public good, by the principle of eminent domain.

But even if you think about a database maintained by a bank, you might think this is a very easy job. I deposit 100 pounds into my bank, the bank just needs to type into a database. In practice, this is incredibly difficult. If you remember, in my first lecture, I talked about how bank systems are written in legacy languages like COBOL. And this has an enormous impact. For example, Wells Fargo is one of the biggest banks in America. It was recently fined over $3 billion because it made a number of database keeping mistakes. What mistakes did it make? Let's take a few examples. If you had an auto loan, for example, but you had a deferment on your auto loan, the bank was supposed not to press you for payment. Unfortunately, the loan deferment database did not talk to the auto loan payment database. So people with deferments got letters asking them

why they had not paid. Similarly, some customers delayed payments to the last day. They called the bank and the bank took that payment and acknowledged the payment. But they forgot to update the repossessions computer who sent out notices saying that the car was being repossessed even after the payment was made. During the COVID crisis, Wells Fargo offered loan modifications to a number of people who had borrowed money to buy houses. For 190 people, Wells Fargo decided they were dead so they didn't need to be offered the loan modifications, but those customers were not in fact, dead. Those 190 people kept sending money to the bank. Now you might think the bank would say, wait a minute, these 190 people are dead. How are they sending checks? Unfortunately Wells Fargo is a big bank, and their systems don't do very well at talking to each other. Databases are tough to maintain and talk to each other.

The final alternative is to trust a whole lot of complete strangers. That is the essence of crypto. Crypto consists of completing transactions between two people without that centralized record keeper, the bank. For example, you could send money, you could write a real contract, you could create a market for people to interact with each other again and again, without a centralized record keeper, but a whole bunch of strangers who are economically interested in keeping all the records safe.

Crypto

Now, as I mentioned in my last lecture, crypto is kind of a general phrase which applies to a lot of different things. For example, you could talk about cryptocurrencies, basically all about money. Or you can talk about tokens which sort of deals with money. We'll talk about decentralized finance, which deals with automatic contracts. You can talk about blockchains, which deals roughly with databases. But this is all under the big term called crypto.

You also have Web3, which is the sort of decentralized evolution of Web1, which is the earliest form of the Internet where Tim Berners Lee set up and Web2, which is taken over by the big tech companies like Google and Facebook. Web3 is a decentralized evolution of Web2.

But how does crypto relate to finance? Finance is bizarre. Our key rules and principles in finance are based on a set of arcane ideas that don't make a whole lot of sense unless you know financial history. So to understand how finance works really well, you need understand the history of how that particular thing evolved.

Crypto is equally bizarre. And over the past 15 years, crypto has built an entire financial system from scratch. It's basically reinvented or rediscovered things that finance has been doing for centuries. Sometimes it has found new and exciting ways to do things. Sometimes it has found worse ways, basically heading down dead ends which have been abandoned by traditional finance decades ago. Sometimes it has discovered similar solutions as traditional finance, but with new names and new motivations now.

Consensus Protocols

Why would a bunch of anonymous strangers want to spend time verifying your transactions? We need to make it economically interesting for them to do so accurately.

But even if a 1000 people all verify your transactions, how do you consolidate those 1000 opinions? Majority rule perhaps? If more than 500 people agree on a transaction, that will be the consensus truth. Unfortunately, that doesn't work because of something called a Sybil attack, not named after the Greek prophetesses, but a book in 1973 about a woman called Sybil with multiple personalities. The idea behind the attack is that if there are 1000 people who have to verify a transaction, you need 501 of them to agree, what you do is you spin up 1000 computers with different IP addresses. And so you overwhelm the 999 people who don't have those computers.

The proof of work consensus protocol makes it expensive for you to spin up 1000 computers in order to create a fake majority for yourself. As you spin up more and more computers, it costs you more money in terms of electricity on your computer time, than if you simply tell the truth.

Sometimes people say crypto is trustless. But essentially all that means is that I don't need to worry about whether the system can be hacked because I can go in there any time and see all the transactions for myself. So, in other words, a trustless crypto system means that most people trust it without actually checking any of the underlying transactions.

What Is a Cryptocurrency?

Is it a store of value? Perhaps, but why is it a store of value?

Well, value in finance comes from two things: The cash flows arising from an asset and its risk. What are the cash flows from crypto? There are none.

All crypto does is to allow you to transfer ownership of one number from one computer to another. Wait, that sounds weird. What does that mean? Well, sending ownership of a number from one computer to another is a difficult problem. Suppose I were to say I'm going to send you the number 95. How do I do it? Well, I can open up my email type and 95 and send that to you. But does that mean I lose ownership on it? No, I can tap into another nine five, just type it in. I don't lose ownership when I transfer one number to you. I still have the number.

Satoshi Nakamoto invented a method by which if I send a number to you, that number is deducted from my own store of numbers. I can no longer use that. And then a group of people said whoa, that's like a currency. Let's assign an arbitrary value to that. That is a connection to the real world. It is a socially acceptable arbitrary value assigned to a digitally scarce number.

But that got interesting for a whole bunch of people who said hey, people are assigning values to arbitrary ways of sending numbers to each other. And they started their own cryptocurrencies. One example is Dogecoin which was created as a joke by software engineers Billy Markus and Jackson Palmer using the Shiba Inu doge meme. It is worth around 6p today. There are hundreds of different types of cryptocurrencies in the world today, but the dominant ones are still Bitcoin and Ether. More about Ether later.

Another way to think about it for finance professionals is that the bitcoin protocol allows you to send a number from one person to another. What is the value of that in the real world? It should be arbitrary. For finance people, this is super interesting, because the value of anything in finance comes from cashflows and risk. But what is risk? For a finance person, risk is all about correlations. That means in other words, if you have assets that are correlated, they're all go down or go up together. So something that does not go down when bad things happen and everything else is crashing, is maybe a good investment? A lot of institutions thought that maybe cryptocurrencies are good investments because they're uncorrelated to anything else. Something like gold, or something like that which maintains its value, in spite of the fact that everything else is going down. Unfortunately, that turns out not to be true. Crypto currencies are somewhat more of meme stocks in the sense that people agree that this is valuable or irrelevant arbitrarily. And the values seem to be correlated with the economic cycle. We'll talk more about that later.

Cryptocurrencies As Distributed Computers

Another way to think about cryptocurrencies is that bitcoin is like a distributed computer. Think about what Bitcoin does. You send a message to the computer, say, transfer five Bitcoin from my address to someone else’s address. The computer does that. But that's the essence of a computer program. It's just has one function, transferring money from one computer to a different computer.

Someone called Vitalik Buterin invented something called an Ethereum virtual machine. The idea was simple. If a large distributed computer is already doing executing one line, which says, send money from A to B, that's the same line which verifies consensus. So what he did was to add an if-then statement.

There are two types of if-then statements. One type would be if something happens, then send money from A to B. But that's the essence of a hedging strategy. You could say, if the pound falls below 1.1 to the dollar by December, then send five ether to Mary or if there is snow England in April 2023, then send to Bitcoin to somebody else. That statement depends on something called an Oracle. An Oracle is a computer connected to the outside world. It tells that Ethereum computer that yes, snow fell somewhere in England in April 2023. Or it might say, yes, the exchange rate of the pound is really 1.1 to the dollar in December.

But the if-then statement can also be a vending machine. If someone sends ether to this address, the program will send you back a picture of a bored ape. That vending machine is independent of the outside world.

The distributed computer has no keyboard, it has no mouse, and it has no monitor. It just runs a bunch of programs called distributed apps, DApps. These are programs that run on the web but keep some data in a blockchain. Think about yourself playing a character in a swords and sorcery fantasy game. Your sword is rendered on the graphics monitor by the graphics card. But the fact that you have a sword at all is data that's

actually kept on the blockchain. So in other words, the program will go to the blockchain and check whether the character is meant to have a sword or a piece of armor, or a helmet, and so on. And so when your character appears in the video game, you're wearing all the armor and everything because your ownership being pulled out of the blockchain.

That's kind of like a distributed app. So if you write a distributed app, what it does is it broadcasts instructions to thousands of nodes in the network. Each of these nodes execute all the instructions. Then the system reaches consensus on the results of those instructions. That means this program executes thousands of times on thousands of computers.

Reaching Consensus on a Distributed Computer

How does distributed computing reach consensus? Well, until fall last year, it was all done using proof of work. That means an enormous amount of electricity was being consumed because each of these 1000s of computers will be solving meaningless cryptographic puzzles in order to grab a block, verify that block of transactions (or in this case execute programs) in order to get to the block verified on the blockchain.

But last fall, Ethereum shifted to a proof of stake system, which is much more efficient. How does that work? Well, you can validate a transaction in on the blockchain by buying the network currency and deposit in a special smart contract, which doesn't allow you to withdraw that money at all. That's called your stake in the system. If you have a stake in that system, you're called a validator. Validators do compile all the transactions into blocks. And at fixed intervals, one validator is chosen to propose a block. Another bunch of randomly chosen validators reviews that block, carries out all the instructions, verifies that these are valid, and then votes. So, this group of validators basically verify the appropriate block and place it on the chain.

What happens if you are a dishonest or lazy validator who does not verify the block properly. If other people find out that you have not been doing an honest job and verifying the block you get properly, you lose your stake.

Of course, there's also the case that you collude with other validators to all take it easy. Then people lose trust in the system and the value of the stake goes down. So there is an economic interest in keeping the verifications honest.

So how do we earn money in these two systems? In Bitcoin, using proof of work, you buy lots of computers, solve meaningless mathematical rules, and earn Bitcoin, In contrast, Ethereum is a proof of stake network. You deposit ether to buy a stake, validate your transactions and earn fees which are called gas fees based on your stake.

It's important to specify just how important gas fees are on ether. Ethereum is much more complicated than Bitcoin. Bitcoin is just a very simple set of transactions, basically sending money from A to B with no conditions. Ether allows you to run a program. If A happens, then do X, But if B happens, then do Y. You could have a long list of instructions built into one transaction. And all of this must be verified. So suppose you get a program consisting of 10,000 instructions, that's going to use up a lot of computing time, because each of those 10,000 instructions have to be carried out on all the processing nodes, which then have to come to a consensus. So Ethereum sets a limit on the amount of gas you can offer to run your program and an amount of gas charged per instruction. So you cannot run a program which goes into an infinite loop and keep churning away until the system is broken. So the gas fees allow us to earn money through our stakes.

Crypto Finance

But this example also allows us to see how crypto is reinventing stuff we know from traditional finance. Think about interest. Why do you earn interest when you deposit money in a bank? When you deposit money in a bank, the bank takes that money and lends it out to other people who are doing more productive activities, and they earn money on their productive activities and return it to the bank. The bank gives you a portion of that earning in the form of interest.

In contrast, suppose you want to become a validator but you don't have the money. You can borrow a bunch of ether from a group of your friends or from a mining pool. Then become a validator with offering the pool as your stake. You earn gas fees from validation and you return some of it in the form of interest. Here there's no productive use whatsoever. All you're doing is validating a transaction on the blockchain. But crypto has reinvented why interest is paid.

Or take starting a company. I'm going to introduce the concept of fungible tokens. Why do you need a token?

Well, let's start thinking about how you set up a business, specifically, a platform or a market. You have a chicken and egg problem. You need both buyers and sellers. If you don't have buyers, you won't have sellers and vice versa. But how do you attract either side without the other one? That's the problem of network effects.

But tokens allow you to start markets without either side being in place. Creating a new token is easy. And there's an Ethereum white paper describing the ERC-20 protocol which allows you to have a 4 line code snippet for implementing a token system.

So how do you raise money for a company? Well, you need to lay out a business plan, go to a venture capitalist or an angel investor, and ask for an investment. The problem is that you have to demonstrate that you will have enough customers for a viable model. If you cannot persuade your shareholders, you will not have enough money to attract customers. But without customers, shareholders will not invest in you. Again, it's a chicken and egg problem. Without shareholders, I can't build a platform. Without the customers, I can't attract to shareholders. How do I solve this?

Ethereum solved this conundrum by creating their own token called ether. If you bought the ether tokens early, you could buy them cheap. If more and more people use Ethereum, that token goes up in value. So, in other words, Ethereum made their customers into their shareholders. That was a brilliant strategy. And a huge number of entrepreneurs thought they could do the same thing. So they all launched so called initial coin offerings, and they were everywhere in 2017. People use coin offerings for everything – they said, "We'll give you a token if you give us money. As more and more people use it, the company will become more and more valuable, and you will become richer and richer because you bought your initial coins cheaply."

Unfortunately, ICOs pretty much died out after the SEC ruled that they were security offerings which means you would have to disclose a lot of stuff and file a lot of statements with the SEC. But there were variants such as governance tokens, utility tokens and so on. The latest form of governance token is something called a digital autonomous organization. A DAO is a group of people who get together to do something together. They put money into a pool, issue a bunch of governance tokens to all their investors and write a contract to invest in something else. There was, for example, a ConstitutionDAO which pooled money to buy a copy of the Constitution.

But this has problems too. For example, in May 2022, a DAO was sued because the people suing said that investing in DAO was like a partnership - there were no articles of incorporation. Unfortunately in a partnership in America, you have unlimited liability. This is bad. Corporations, in contrast, do not have unlimited liability. They have limited liability, which means that the maximum you can lose is the amount of money you put in. But if you don't think about these issues, you end up yourself finding yourself in an unlimited partnership, which is much riskier than a corporation.

Let's turn to non-fungible tokens. Tokens can be unique as well. How? Answer Ethereum protocol ERC 7.1 which added a token id to a contract, so that each contract/token id is unique.

All this is a program which will go to a website or a database with a unique number, a token id. The database is full of images. If you have token id one, we'll go take that first picture out and send it to you. And remember, you own that token id. If anyone else sends the program with the token id, they will get the same picture but with a note that you own the token.

This became incredibly popular. For example, Beeple sold a non-fungible token for $69 million. Before that, you know, the maximum price he'd ever got for a single piece of artwork was $100. In contrast, you will could buy a real-life painting of Monet's water lilies for only $54 million at auction. Similarly, someone bought a cryptocurrency cat for $172,000.

Remember all this is a line in a smart contract, which says I have bought this number on this contract. So when I execute that contract, it takes me to a location on the internet and serves me up a picture of what you bought. It doesn't mean anyone else can't use it. In fact, a lot of people took advantage to this. There was something called the Global Art Museum, which launched NFTs on the Mona Lisa, Sunflowers, and a bunch of other famous paintings. Remember they don't own the paintings, all they did was to write the program. The program will go automatically to the Louvre's website and serve up a picture of the Mona Lisa. There was also a lot of insider trading. The Bored Ape group of NFTs is a very popular group of NFTs. Insider trading allegations were made against someone called Nate Chastain who worked with Opensea that released new Bored Ape images every Monday. Nate bought them pre-launch and sold them for higher prices on the launch day.

This all might sound weird. But let’s see how this might be useful. Let’s reinvent secured borrowing. How do you borrow money using a secured asset like a house in the traditional finance world? You might go to your bank and say you have a house that you'd like to borrow money against, basically a mortgage. The bank sends an appraiser who values your house and the bank lends you, say, 50% of the value of the house.

But now let's say you want to do this in the crypto world. How do you do this? One possibility is something called martingale fractionalization. That's another protocol on the Ethereum blockchain. Let's suppose you want to sell 50% of your house. But you don't want to use a bank. What you do is you launch a NFT of your house. That is a pointer pointing to your house, to your title deed of your house on the internet.

Someone buys it and you get some money. The purchaser has bought a 50% value of your house, but your house is the whole house. You don't want to move out of it. You can't sell 50% of your house. Well, let's go on to the end. Let's say five years from now, you decide, okay, that time has come, the payment is due. I'm going to have to give 50% of my house. How do you do it? Well, you roll a die. If it comes up 123, you lose the entire house. But if the die comes up 4,5 or 6, you keep the entire house. In other words, you have sold 50% of the expected value of the house. Now you don't have to go through with the deal of course. Your NFT is one of a class of equivalent houses. It's an NFT pointing to your house, but you can replace this with an NFT pointing to a different house, which might be something within the London area. What you can do is just before the contract comes due, you buy that NFT to the other house and you replace your NFT with that other NFT and so you don't actually have to sell your house at all. You just have to pay the market value of the other NFT.

Can Blockchains Be Useful in Business?

There is unfortunately a problem in crypto called the blockchain trilemma, which was described by Vitalik Buterin. Three things are necessary for a blockchain to be useful: Security, scalability and decentralization. The problem is, you can only achieve two of those three things. For example, you take traditional chains such as Bitcoin or ether, they are secure and decentralized, but they're not scalable. Similarly, you might think of decentralized and scalable chains on multi-chain ecosystem, but they're not secure. They have been hacked lots of times. You can have scalability and security. That means you have one core network, basically controlling everything on its own chain, but that's not decentralized. There are companies trying to solve the problem. For example, there are layer 2 protocols in Bitcoin and so on, but these are beyond the scope of this lecture.

And of course, regulators have problems with this. Suppose your regulator comes to you and asks how you are maintaining the security of your databases. And you say ah yes, I've got some random mining pools in Russia, and they're verifying my transactions. You can bet your regulators are not going to be happy.

One way out is to start private permissioned blockchains. So for example, a group of banks might get together and say, Hey, the 10 of us know each other very well? Why don’t we set up a private blockchain, between the ten of us. The only people are allowed to sign in the blockchain all know each other. That's been the approach taken by a group of different companies. Maersk did this for shipping transactions, R3Corda took this approach for banks. Not all of them worked. Maersk recently announced that their system was being abandoned. Australia’s stock exchange abandoned a years-long plan to upgrade its clearing and settlement system to a modern blockchain-based platform after a series of delays.

Moving From the Crypto World to the Real World

Moving from one blockchain to another is tough. I might hold Ether, but I would like to exchange it for Dogecoin. How do I go from ether to Dogecoin which is on a different crypto network? What do I do? Well, one possibility is to send my Ether to a crypto bridge, a secure address on the Ethereum blockchain. The address notifies an off-chain computer which calculates the value in Dogecoin and sends it to your address on the Dogecoin chain. That's tough but doable.

Moving between the blockchain and the real world, that's much tougher. Houses are not digital, houses burn down, get damaged, are improved. How does the blockchain reflect these changes in value?

The crypto world is an intricate, completely self-contained system of permissionless innovation. I don't have to ask anybody's permission to launch a contract on the blockchain. I don't have to ask Vitalik Buterin’s permission to launch a smart contract on Ether.

So there are two views on crypto: One, it is a streamlined modernized innovative evolution of traditional system or two, it is a chaotic devolution of the traditional financial system that has never learnt important

lessons or lessons about fraud, leverage, risk and regulation.

Let's take an example. Who is responsible if you make a mistake? Suppose you lose your password to your online bank account. The website usually gives you lots of alternatives – if you forget your password, click here. Or you can call the bank and ask them to reset the password for your account. And the bank might ask you for verification and say okay, fine. The password is test123, don't lose it this time. But what happens you lose your private key? There are lots of examples. Like for example, this poor guy living in San Francisco, who had his private key to 7000 BTC (about $200 million) stored on a secure hard drive called IronKey which allowed you to have 10 guesses before seizing up and destroying the password forever. What would you do?

Investing in Crypto

How can *you* invest in crypto? Well, if you are a mainstream institution, you might think of a Bitcoin future. A futures contract does not actually require you to own the asset. In an oil futures contract, I can take a bet on the price of oil without ever owning oil. So, I can do the same thing here. A futures exchange sells Bitcoin futures. This is a very well established traditional financial process so a lot of mainstream investors said that's the easiest way to invest in crypto.

But lots of ordinary people don't know how to use futures. No problem. You can buy a futures exchange traded fund. This is like a stock. So you have a stock wrapper put on a future which in turn is put around a Bitcoin.

Can you buy crypto through an exchange yourself? Yes, you can. You can apply to a crypto exchange like Coinbase or even Revolut in the UK. They will sell you crypto but what's the problem? Well, suppose I ask them to send me a Bitcoin and I allow them to charge my credit card about $17,000. So the bank charges the credit card and sends you the Bitcoin. Then when you get the Bitcoin, you call your credit card issuer and say your card has been hacked. I never bought any crypto. The bank would reverse the charges, and possibly get the money back from the exchange. So if you buy bitcoin from an exchange, in most cases, you're not actually going to get that money. It is going to be held at the exchange. That's safer in a way because the platform has your private key. That's called managed custody.

But there is still a big problem. Who guards the guardians? Exchanges have been hacked. A lot. Mt Gox was hacked and lost 850,000 Bitcoin. Some of the cryptocurrency has been recovered. For example, the Bitfinex hack resulted in a recovery because the problem is again, moving from the crypto world to the real world on the crypto world because every transaction is recorded. You can trace the flow of money going from the original theft to a wallet A to wallet B and so on. But as long as you stay in the crypto world, you are safe. But how do you get that money out? And in this case, the perpetrators were caught because they bought a $100 Walmart gift card with crypto and had it sent to an identifiable IP address.

Crypto and Exchanges

How do crypto exchanges work? A regular financial stock exchange is straightforward. I can borrow money to buy stock. Specifically, I lever up by getting a margin loan, putting down only a small value in my account. If the price of the stock goes down, I get a margin call from my broker. My margin account usually keeps contains enough cash that I don't feel tempted to run away and leave the value in the margin account for the broker to keep. Crypto exchanges sort of work in the same way. But they have to take a lot of very centralized decisions. How does it set the leverage limits? Bitcoin fluctuates in value a lot more than a security does. What collateral is allowable? That is a lot of centralized decision making for a decentralized network.

But the basic margin loan idea can be developed into something called stablecoins. A stablecoin is a token that's supposed to be always worth $1. How do you create something like that?

One simple approach is something called a collateralized stable coins. An example is Tether. Tether claims that if you give it $1, it will give you $1 worth of Tether. It keeps that dollar in a safe in an envelope with your name on it. And when you want your money back, you return the Tether and it will pick your dollar out of your envelope and give it to you. Of course, they won't make that much money using that exact system. So, they actually lend out that money. The problem is if you lend out the money and post the loans on a blockchain, people can see exactly how much money Tether has and where it is invested. And that can create problems such as bank runs. So Tether keeps talking about how all its accounts are audited to prove that it has the money to pay back all the depositors, but they never actually reveal any details.

A more sophisticated approach is an algorithmic stablecoin. The idea here is exactly the same as a margin account. You put in $100 and you receive a token that's worth $100. But you put in a large amount of cryptocurrency in your margin account, way more than the value you have borrowed, so the large volatile cryptocurrency is stabilizing the value of the algorithmic stablecoin. Your deposit is like a senior claim on the cryptobank's assets. Basically, you get paid first before everybody else. There are fancier versions involving two

coins. But sadly, most of these have been involved in death spirals, a name which is just as bad as it sounds. A famous example of a death spiral is TerraUSD/Luna.

So how do crypto exchanges work? In a regular stock market, we have market makers who use a central limit order book to keep track of orders. For example, if you place an order to buy shares at, say, $100 per share, the market maker puts that on his books and wait for a sell order to come in at a price lower than $100. When the second order comes in, the market maker nets two trades off against each other and closes the order.

Unfortunately, this doesn't work in smart contracts. The reason is because every time you place an order, even if the order is withdrawn later, another instruction has to be sent to the blockchain. So you have to pay high gas fees even if your order is never fulfilled.

Crypto has come up with a brand new way of market-making, which is very different from anything found in traditional finance. It uses automated market makers and an algorithm for keeping the order book. Let's take an example of such an algorithm – the constant product market maker rule. The market maker first deposits equal amounts of, say, ether and $1 equivalent stable coin, say USDC. IF the current market price of ether is around $1,200, the market maker deposits 1000 ether and 1.2 million USDC into the pool. All the algorithm does is to keep the product of these two numbers (1.2 billion) constant over time. For example, let's suppose that someone wants to buy 100 ether. That leaves 900 Ether in the pool. To keep the product the same, the market maker must increase the number of USDC in the pool. How much USDC should there be in the pool? Well, 1.2 billion divided by 900 is 1.3333 million USDC. The pool already has 1.2 million USDC which means another 133,333 USDC needs to put into the pool. That is the exchange rate, in this case, one ether is 1333 USDC.

Finally, let's talk about arbitrage and crypto. Real world arbitrage is tough to do. Even when you come across an arbitrage opportunity, you probably do not have the resources to exploit it sufficiently. Decentralized finance is new enough that pricing anomalies exist is also efficient enough that everything happens visibly on a virtual computer running public code. So, you can reliably exploit these anomalies. How do you do this? The answer is through flash loans. Flash loans are basically a set of computer programs which involve buying and selling the same asset with different prices across multiple exchanges. The key is that all the programming instructions are written in one program - one transaction that executes all at once. If any part of the transaction is not valid, the entire program is never executed. In other words, the program exploits the arbitrage opportunity *only* if the arbitrage is likely to be successful.

Flash loans have been used to take advantage of mistakes and smart contracts. Basically, somebody writes a contract which has a bug that occasionally lets a user put in one token and get back to somebody else notices and writes a program to use flash loans to put in a billion tokens and get back 2 billion tokens and blow the smart contract up entirely.

Are there any other problems with crypto? Yes, front running. In traditional finance when you place an order, your order goes to a broker who routes it to different exchanges at different times through different pipes. Flash traders might try to exploit this but it's difficult for them. In crypto, this is explicit. If we find an arbitrage and send some orders to a decentralized exchange to do that arbitrage, an arbitrageur can see those orders in the network and send the same order to the exchange but with higher gas fees. She gets priority over you so that the trade is done before you have a chance to exploit the anomaly for yourself.

So how can we sum up? What is the future of crypto? The big problem crypto faces is how to associate the crypto world with an asset in the real world. This is extremely difficult to solve and may even be potentially unsolvable. It's much easier to think of digital assets connected to each other through crypto. You can think of communities like the metaverse, which are entirely digital, and perhaps trust will migrate from the real world to a digital world. In that case, crypto might be useful, but at the moment, it is difficult to figure out how to use crypto in the real world.

References and Further Reading

Lewin, Matt, 2022, "The Crypto Story" in *Bloomberg Businessweek*, Oct. 31, 2022. Available at https://www.bloomberg.com/features/2022-the-crypto-story/