Tholus Capital web3 investor podcast

Episode 1: Blockchain technology with Gil Rosen

Transcript

MARKUS FEDERLE
00:19
Welcome to the Tholus Capital Investor Podcast, the podcast for investors on all things blockchain and Web3. Brought to you by the team at Tholus Capital, we provide global investors with insights into blockchain technology, its practical application, and its potential as an investable asset class. This is a show from investors for investors, including those who are new to the asset class. It's time for investors to take a look at blockchain technology. And we are here to deliver just that. This is the Tholus Capital Investor Podcast, and I'm your host, Markus Federle.

DISCLAIMER
01:06
Markus Federle is the founder and managing partner of Tholus Capital, a global investment firm focused on blockchain technology and web3. All opinions expressed by Markus and podcast guests are solely their own opinions and do not reflect the opinions of Tholus Capital or its clients. This podcast is for informational purposes only and should not be relied upon as a basis for investment decisions. Tholus Capital and its clients may maintain positions in the securities discussed in this podcast.

MARKUS FEDERLE
01:42
Hello and welcome to this inaugural episode of the Tholus Capital Investor Podcast. We are here to take you on a journey through web3 Venture Investing. Before we delve into the depth of web3 investing, we want to make sure we have properly understood the technology which is at the core of this new industry. And this is why we will dedicate this very first episode of our Investor Podcast to the basics - the blockchain:

What is blockchain technology?
How does it work?
And what is so novel about it?

In other words, we will focus on the conceptual foundations of the technology and lay the semantic groundwork for the discussion ahead. Without going too deep, we will explain the meaning of some of the frequently used key technical terms and their significance for the technology. To help us answer these questions, my guest for this very first episode of the Tholus Investor Podcast is Gil Rosen.

Gil is the president of the Stanford Blockchain Accelerator and a lecturer in blockchain entrepreneurship at Stanford University's School of Engineering. He's also the managing partner of the Blockchain Builders Fund and has invested in over 50 ventures across blockchain, fintech, digital health and sustainability. Last but not least, Gil is a senior technology advisor at Tholus Capital. Please enjoy my conversation with Gil Rosen.

I'm very excited today really for two reasons. For one, it's our very first Tholus Capital Investor podcast. And two, we have Gil Rosen from the Stanford Blockchain Accelerator here to explain blockchain technology to us. And given his background and experience, I honestly cannot think of a better person to do that. Gil, thank you so much for joining us and welcome to the show.

GIL ROSEN
Thank you, Marcus. Appreciate it. Excited to be on the show.

MARKUS FEDERLE
03:41
Now, before we dive into the technology side of things, as with all of our podcasts, I do wanna ask you about your personal journey into blockchain, or shall I say, in and out of blockchain and back, because I really think there is a fascinating story here. And of course, we do wanna hear about your Stanford Blockchain Accelerator and what you guys are doing there.

GIL ROSEN
Awesome, thank you. Yeah, it's been quite the relationship with blockchain. So I guess... quick like 30 seconds before that my background in general is from the distributed compute space and leveraging technology and specifically distributed compute platforms and data infrastructure to build enterprise applications for industries. So I first came upon blockchain technology actually when I was at business school over at Stanford in 2016 and kind of began to see the possibilities for at that point what I thought was more marketplaces and transactional systems that were truly shared and owned by users. And to me, that was exciting. There was a lot of hype around the potential there for blockchain, both in revolutionizing financial systems, but also kind of all of these marketplaces that we saw popping up, whether it was Uber, Airbnb and others, and how they could potentially be owned and managed by users and stakeholders.

And that excited me and I started kind of supporting and advising and investing in a whole bunch of projects. I started a hedge fund, but I think the openness of the technology itself also allowed for a lot of bad actors and there were a lot of scams and rug pulls. There was a lot of insider information and ultimately I did well, but I think I was turned off by the amount of just the noise in the space and, and really the technology was early. There was a lot of promise and people were raising a lot of money for many projects that didn't exist and they needed time to build them. And one of the challenges with taking any technology company and putting it in a public market is that it's subject to public sentiment.

And if we look at even biotech companies, when they go public on the stock market, it's a lot of hype. They pop, they drop. It's based on news as opposed to being based on fundamental value of what's actually there.

And we saw the same thing with blockchain, where you'd have these amazing projects that were based on research or ideas with strong people, or at least seemingly so, go public. And then it's based on sentiment and the price would pop and drop purely based on someone's news, someone saying something word of mouth, as opposed to real fundamental value, because it takes years to actually build software and to build products.

So I felt both that the fundraising environment was a little bit early as well as the technology itself was very early. And I actually took a step back and went into general investing of technology and data infrastructure for emerging market fintech and digital health and sustainability and supply chain and energy and a number of other verticals.

About two years ago, I went back to Stanford for another degree in public policy and I started to see exciting projects that were building like real applications and technology to solve a lot of the challenges that blockchain had, both in terms of its ability to actually create applications that we can use, but also usability, performance, and they were building real technology.

A friend had at that point started a blockchain accelerator because Stanford is this amazing place for innovation where in my year alone, I think there were over like nine unicorns that came out of that year. And in tech perspective, we have tons of accelerators, but there was nothing that was blockchain focused specifically. And fundamentally, building in blockchain and going to market in blockchain is quite different than in the traditional venture space. Again, between tokens and crowdsourcing, building decentralized technologies that are really ecosystems in marketplaces to coordinate between different parties.

So initially he asked me to help out as a mentor, and then I ended up being asked to run the accelerator itself. And the mission of our accelerator is to really help drive broad blockchain adoption. So we incubate about 10 to 12 teams from either Stanford student or alumni, only bring on teams that have technical founders, where the teams themselves are tackling the frictions within blockchain itself. So it's a lot on the infrastructure sid to ensure that the technology is really performant, scalable, interoperable, cost effective. There's a lot on the usability side to ensure that people themselves are able to interact with blockchain technologies in a way that they don't need to know that they're interacting with blockchain technologies. Just like when I'm using my banking application, I don't know that there's an API behind it. I just know that it works. So it just works and the user experience is significantly better. The developer experience is better as well.

After we incubate these teams, the three partners who run the Accelerator are also investment managers that support these teams directly and provide capital within their earliest rounds alongside some of the leading funds in the space in Driss and Sequoia, Bain Capital, Gumi Crypto, Dragonfly, et cetera.

MARKUS FEDERLE
And I think that's actually a fascinating story in a way, because you were early on quite intrigued by the technology, but at the same time put off by all the noise and the hype around it, only to come back to a much more sound environment for developing the technology a few years later. So let's come to the core of today's podcast. And that is of

course, blockchain technology. The reason the team and I decided to start our podcast series with an explanation of the technology is that we feel that even though there's a lot of information on blockchain out there, and almost everyone has now heard and read something about it, there also seems to be quite a bit of misinformation and misunderstanding. In particular, in my experience, the debate about blockchain sometimes seems to be quite an emotional one. And that's from both sides. Pro and con. And of course, some of that has to do with the reaction people have to cryptocurrencies, which is an important but only one of the possible applications of blockchain technology. And that is really a peculiar thing that people are having an emotional reaction to a technology. So I really think it's time to take a step back and take a sober look at the technology to understand what we are really dealing with here. So without further ado, over to you Gil, what is blockchain and why is it important?

GIL ROSEN
So in its simplest form, blockchain is the first truly shared data store that setting everything else aside, it's a technology, it is a shared data store. And until the Bitcoin white paper, this really didn't exist. So think of it as a ledger or a database that you can only add data to. You can't ever change anything in the past, which is important for transparency traceability. And it's based on this novel mix of cryptography, distributed computing, and economics to incentivize multiple players to really operate this shared data store. So let me again, take a step back here. If you think about every application that we interact with, whether it's our banking applications, our healthcare records, literally any app on your iPhone, any company you work with, it's all owned and managed by a single party, whatever company that you're interacting with, Facebook, Instagram, WhatsApp.

Your health records are also sitting in a database that's owned and managed by your insurance provider. Your music sits on Spotify servers. And you interact with their application specifically, and they control permission access. They control what you can do on it. They control what you can build on top of it. And if you wanted to build an application to do something novel, by and large, that's not possible. You can't build an application to manage your own health records on your health insurance's platform, you can't just build a fintech application by and large.

And it makes sense, because someone needs to physically own and manage computers and servers, and someone needs to own and manage the applications and maintain them. And someone needs to be accountable to their commitments and responsible for their performance for their security. So you pay them in one way or another, whether it's through advertising dollars or directly through some sort of subscription service or transaction fees and they provide you and us with a service. So there's both pros and cons to this. And that's the entire world of applications that we know today and the internet is run and managed by private companies.

In the physical world though, we have this concept of shared infrastructure, right? So we have money that we can physically hold and give people and we don't need to rely on anyone else for that. In the digital world, someone needs to keep track of your money and send it to people for you because how do you prove this ownership of money in the first place? So someone has custody and defines that, and it's a pain to physically give money to someone across the country. So we let banks manager ask, but it means that we rely on these third parties to hold our money safely. And again, that's true for like every application that we have. We've seen with the SVB debacle that banks can always be trusted. And this was especially true post 2008, which was actually one of the things that drove interest in Bitcoin and the creation of Bitcoin in the first place. If you wanted to open a financial platform for storing and exchanging money, how can you do it without banks? Or even if you wanted with banks, what does it mean to have a shared database with bank account information? Who manages it? How can you trust them not to change records through malice or incompetence? And most importantly, how can you ensure that funds don't get stolen? Who's going to physically hold money? So Bitcoin was this attempt to build a shared application that could be used to store and exchange money. But its novelty and potential isn't just in storing money and moving money and financial transactions, which is I think how many people see it as cryptocurrencies. Its novelty, this idea of a shared application period that has tremendous ramifications for our economy and how our society interacts.

MARKUS FEDERLE
So, Gil, I mean, how does this actually work? It's a shared database. There's no one I should trust or need to trust. So what am I trusting? What's going on here?

GIL ROSEN
So we can think of Bitcoin as this shared database where instead of Amazon or Google or your bank owning and managing servers and updating records, what we're using is a redundant platform that you have thousands of people that they themselves make all of these updates. So let's call all of these thousands of people that are making these updates and running the platform miners. Basically, if someone in simplified form, if someone wants to send a transaction. Instead of them asking their bank to do it, they send it up to this network of miners, and you have thousands of miners that then receive this transaction. They're split up into groups, so to speak. One of those miners then actually goes and creates a block of new transactions that are proposed and the miners around them can validate whether that's true or not. And there's this consensus mechanism to determine if a block is accurate or not.

Now only validated blocks are ones that are formally added to the blockchain and people continue to add blocks to the longest validated blockchain. Now, in theory, someone can go and create thousands or millions of fake transactions, and perhaps they can fool enough of the people around them into thinking that one of their blocks is accurate. So to prevent this and to prevent fraud, there needs to be some sort of cost mechanism. And that cost mechanism is where this concept of proof of work comes in where there's an energy requirement and energy costs money in order to propose any new blockchain. And that's kind of where the term mining comes from. So basically, every time you want to propose a block, you need to guess a hash beneath a certain hash number. So you're constantly generating these random hashes and that is very computationally expensive and once you actually find that and you've spent enough energy, then you're able to actually propose this block. Because of that, people have created special servers called ASICs that are able to actually perform this in a more effective and efficient way. But ultimately, the aim of all of this is just to ensure that there's a cost that's incurred. So that if you're creating millions of fraudulent transactions, well, actually, that's going to cost you a significant amount of money and you're disincentivized from doing so.

16:56
However, if you propose a block and get chosen and your block is validated, then you reap a reward. The rewards have been having every few years, but ultimately you're reaping a reward here for operating as a miner. So really what we're doing is we have two groups of people. We have users like you and I that want to perform transactions, and then you have miners, and the miners take the place of Amazon or AWS or Microsoft Azure or Google Cloud. And the miners are permissionless, which means anyone can be a miner, but also the network is permissionless. So anyone can make transactions. So because anyone can be a miner, we wanna incentivize miners to perform these operations of proposing transactions and updating transactions. And in essence, because you have thousands of people redundantly doing and validating each other's work you can ensure that it's true. And we use these concept of hashes, which basically take an amount of data and convert them into this short code that only that real input data can create this code to almost use it as a timestamp to validate that everyone's data is synchronized. So we have multiple people redundantly validating transactions. We have everyone constantly synchronizing their database with each other.

18:23
And in doing so, we've created a shared database that doesn't rely on any specific third party to manage and own the servers. That's in essence, unhackable, unless you can take over more than 50% of your servers.

MARKUS FEDERLE
Great. So let me just recap this for my own sake. So previously I was trusting one person. That could be a bank. It could be a person running a central application. And now with blockchain, I am basically trusting a network. And the network is a multitude of nodes that are run by miners. And these miners have an incentive to do work to validate the transactions on the blockchain. They're checking on each other. And in order to game the system, I would actually have to corrupt half of the miners out there.

GIL ROSEN
Exactly. Yeah. And they have to cryptographically prove and can cryptographically prove that they've performed their work correctly and that everyone else has synchronized using these kind of cryptographic hashes that are stored in a miracle tree, but that's getting too much into the weeds there. So what are these use cases and where do shared ledgers make sense for things other than cryptocurrencies? So basically anywhere where you have multiple parties interacting with each other and that need to coordinate with each other, instead of necessarily having a third party ledger for that can have a shared ledger that's shared and managed by the users in the ecosystem.

So this makes perfect sense for something like health records where you have providers, health insurance companies, patients themselves, others that might want to coordinate with each other. Now we're still a long way from health records being a reality. This has been an idea for some time now, but ultimately the idea that you don't need to rely on a third party to have your health record that you can own your health record and everyone can have permission to access to it, it would be incredibly valuable. It's great in supply chain and there are some companies that are already doing this across Latin America and Africa and the continents where you have multiple parties who are updating where the specific item is. Back in my days working in data infrastructure we were using EDI messages to send back and forth for people to know the update of a given status throughout its supply chain of all of the different parties from manufacturers and multiple manufacturers to vendors. It would be a lot easier if they were all using a shared database. But again, in the prior world, who owns that shared database? Until now it's third parties or again, a Google or Amazon. Or if you're really large than like a Walmart.

21:07
But even Walmart has actually been using blockchain for some of these use cases. And really any marketplace in general, whether it's Uber, whether it's Airbnb, or whether it's a regular marketplace for things. Again, these are, it's a place where people can put information, people can create these transactions and it's shared and owned by everyone instead of having one party necessarily manage it and control it.

MARKUS FEDERLE
Now that's understood. Ledgers can obviously have a multitude of different applications. You can store information, you can have a consensus mechanism around who owns what. But let's come to something that sounds far more exciting than a ledger, and that's smart contracts. And the term smart contract seems to suggest something that goes far beyond the simple storage of information. Now having been a lawyer in my previous life, the term contract really speaks to me. But what is a smart contract? How does it work? And how does it relate to the blockchain?

GIL ROSEN
So this was an amazing innovation. He was a teenager at the time when he wrote the Ethereum white paper, but Vitalik Buterin took a look at this idea of a shared database and thought, okay, we have the shared database for financial transactions. We could potentially put other things on the Bitcoin blockchain. And people were thinking about doing that and looking at that and use it for storing assets as well and defining ownership of assets. And Georgia, the country went and put their land registry on the blockchain. But Vitalik looked at this and thought, well, actually, what if beyond just simple transactions, you could actually create a computer and a global computer. And initially, Bitcoin does have smart contract capability. But if you try and encode in the Bitcoin language, it's fairly restrictive in terms of what it can do. So he thought, what if I could create a computer, like a global computer that would create all of these truly shared applications that could do anything? And he went ahead and that's exactly what he did. So he wrote this global computer, it's called the Ethereum blockchain. And in a similar way, you have, at that point it was miners, now it's moved on to validators. We can get to that in a minute.

23:28
But at that point you had miners where instead of just updating a ledger or doing some sort of small computation in a smart contract that then others around them would validate, you could basically write full applications in this programming language called Solidity, which

was JavaScript-like. And really that enabled this concept of decentralized applications overall. Now, instead of just updating information on health records, on ownership of assets such as housing, cars, et cetera. You can actually write full applications that people can use. And the first application that became really popular was Uniswap. And Uniswap was an exchange for cryptocurrencies. So I love this because it was both a really valuable application that could show that with a few simple lines of code, you're able to create an entire exchange similar to the NASDAQ or the New York Stock Exchange or the London Stock Exchange, you're able to create this exchange that's not owned by a third party and controlled by a third party that has specific working hours, but that's completely decentralized and is owned and managed by the parties and that creates incentives for the individual parties within the application to participate within the application. The details of that in terms of liquidity pools and being able to provide rewards, that's, I can save that for another day.

But this idea of a shared application was revolutionary and a global computer was revolutionary because now every application that we have, that we interact with could potentially be decentralized. I'm not saying it should be, but it could be. And that changes how we can interact with each other at a fundamental level. But coming back to the network, because these blockchains are also some of the longest running networks. So talking about network security, you obviously have databases that are sometimes down, they're prone to error, they're run by one person, they can be corrupted. But some of these blockchain networks, because they have so many nodes and they rely on so many people actually running and maintaining them, aren't they some of the most secure and longest running networks on the planet? I completely agree. And again, you have literally thousands upon thousands of people redundantly storing this blockchain information, the entire database information and continuously synchronizing with each other and improving cryptographically that they've updated these transactions properly, which in essence has created this tremendous database system that has been by and large unhackable, at least from the Bitcoin perspective.

MARKUS FEDERLE
So I want to change the discussion a little bit and come to a term that is intrinsically linked with the discussion about blockchain and that is: tokens. And of course we encounter tokens as cryptocurrencies, but there's a lot more to tokens and there's a lot more different functions to tokens. So what are tokens and what are they good for?

GIL ROSEN
Tokens have a number of different uses. And before we get into tokens, I mentioned that we have these two types of parties. We have users and we have miners validated, the people that are running the infrastructure. Users currently are represented by wallets. Right. And a wallet is really just an address or you could think of it as an entry in a database for a specific person or entity, or if it's a program in Ethereum, you could have a smart contract wallet. So it could be like a program. And those are what wallets are these things that can hold tokens, they can hold value. And these tokens, there are a number of different types of tokens. So a token can represent value like Bitcoin.

27:13

It can represent a thing, an object, a digital asset or a digital representation of a physical asset. So it could represent a health record. It can represent your house. It could represent a song. It could represent a picture of a monkey or it could represent a car and ownership of a car. But the idea is that a token is a thing that represents an object, digital or physical. A wallet is a place where you hold and store that thing.

27:41
And again, in this infrastructure that we have, whether it's the Bitcoin, blockchain, or the Ethereum or other smart contracts or global computer types of blockchains, they each need to operate and in order to operate, they try to incentivize their miners, their validators by paying them a token. Now in Bitcoin, that token is also what's used for actual financial transactions in other ecosystems and blockchain ecosystems they can represent different things. So by and large, we see three uses for tokens. The first has been fundraising. I'm building a project. I need money to pay my developers in the traditional venture world. This would be done through venture capital money. So the idea here is, well, why don't I create this token, sell this token to a whole slew of people who in the ideal world, let's call them my future users.

28:39
So they pay me upfront and it's kind of like this crowdsourcing crowd sale. They pay me upfront. I give them this token. I build my platform. And in the future they can use this token on my platform. So if I were to build a decentralized Uber, for instance, I can sell a whole bunch of tokens to people that would either potentially be riders or drivers. And I would then sell this token to a whole bunch of people with a promise that I'm going to build a decentralized Uber. And then,

29:09
Once I've actually built it, then these users can use these tokens to actually ride from one place to another. And because new users would be buying these tokens, there's a liquid marketplace for them. So we create this liquid marketplace and it will be publicly traded so that anyone can buy these tokens and then drivers would be paid by these tokens. So now I've kind of combined two types here. One is the fundraising aspect of a token. And the second is incentives.

29:38
So we would want in this Uber example, drivers to drive. So we would pay drivers a token and that token could have a variable price, just like we have with Uber. We would want riders to ride. So riders could buy these tokens at whatever price the token would be based on supply and demand. And you could kind of do all these things to incentivize more riders and more drivers matching supply and demand. And then we have this third party now, which is the infrastructure layer of these miners or validators who are actually running the application layer itself, and we would pay them with tokens to incentivize them as well. So now we're able to create this incentive structure to coordinate all the parties, the riders, the drivers, the miners or validators to actually work with each other and create this application that again isn't owned or managed by a single third party. You could also use these tokens to pay developers to develop new features potentially for this application. So we can use it for fundraising, we can use it for incentives to incentivize and coordinate across all of these

different parties to work together. There are pros and cons in that, we can get to that in a minute. And lastly is this concept of digital ownership and that's the NFT's non-fungible tokens. So until now if you're fundraising or if you're building incentives you want a fungible token. What does that mean? That means it's like an Amazon credit that you would have, or an Uber credit that you would have, that all of them are basically the same, and you just want people to exchange them. But because we have this shared ledger that everyone can see and everyone can use, we're also able to create this third type of token, which is a non-fungible token. You can show that this specific object is owned by this specific wallet. And that's what an NFT is. An NFT is this concept of digital ownership, which again has never existed before because we've never had a shared ledger before. So digital ownership can be of regular tokens of value of money, or it can be of again title, a house, a car, a specific song, a specific piece of artwork, a health record, or anything of the like. It could be a security and there's tremendous uses in security. It could be of potentially even commodities and you can a farmer can show that he's grown x bushels of wheat and show that this specific bushel of wheat is owned by him and he's created it other people can validate it and then people along the supply chain can show that actually this specific bushel of wheat has traversed this entire path and we see all of these use cases within the supply chain space for blockchain so we've got these three primary use cases fundraising coordination among different parties and NFTs.

Now these are all amazing and powerful. There's also room for a lot of challenges within these use cases. And on the fundraising side, one of the things that kind of turned me off initially was all the scams that happened because people would fundraise and then they'd make a crap ton of money from fundraising and then they just stopped working on a project, right? It was a lot of hype building. And how would you know if someone was actually going to be building a project that they said they would and there's a lot of risk there. So even if they had built a project, again these tokens were going and being listed on public exchanges, which means that the value of the token is floating based on public sentiment before a project exists, so you'd have a lot of hype and a lot of drops. And I personally don't believe, and I think markets have shown, that by and large tokens or securities for projects and platforms that haven't proven product market fit ends up becoming very speculative as opposed to having true fundamental value because it's difficult for the public to understand that true fundamental value. But they do work very well for projects that have launched and have users just like they work very well for large publicly listed companies that have consistent revenues, profits and growth.

MARKUS FEDERLE
So Satoshi Nakamoto's white paper of course was from 2008, which is a while ago, if this is such a wonderful technology it should be everywhere by now. Why isn't this happening?

GIL ROSEN
So the technology and the promise of technology is incredible. Again, shared applications means multiple parties can coordinate with each other and not rely on anyone else. This concept of actual digital ownership or ownership of digital things, which never existed before and now does exist, has tremendous ramifications for us actually owning our own money instead of when, you know, we want to make a financial transfer, we ask banks to do it for us, right? They own our money, they hold our money, and we ask them to kind of

move our money for us, and they move it to someone else's account that they also own. Or if we want to make trades and securities, right now, everything is kind of locked into these specific trading platforms and exchange and brokerage platforms versus us being able to use one asset for margin and another asset.

So the potential is really incredible for ownership for shared applications. But the reality of the technology is that it's like we reinvented the computer as a global computer and it's at the level of a programmable calculator. It sucks. It's slow. It's expensive. It's inefficient. It's really hard to build on. You need to know solidity or rust. There are plenty of things you can't do. They're not object oriented. It's really difficult to use. Again, you have this concept of wallets that represent you, but that means you need to now own this wallet and remember a key that's your key to be able to open this wallet. And if you lose it, you might lose access to your whole wallet, which has happened to many people. So programming solidities of pain programming in the Bitcoin stack language is a nightmare and it's hard because we're building this huge shared computers and if you want to make changes and updates to this computer platform, you also affect everyone else that's using it. Right? So it's also difficult to make these changes. Even more so, if I'm running an application on Ethereum, the cost of my infrastructure is actually dependent on other people running their applications as well. Because gas fees and the price of Ethereum is based on overall demand. So let's say I'm running a health record application for providers to kind of store health records, being able to update health records and share health records and someone else is running a game where they have digital objects that people can play with and their game is really popular. All of a sudden they're gonna be using all the Ethereum compute resources and the gas fees, which is like this Ethereum that you have to pay to use the platform, which is rewards our validators and our users, that skyrockets.

36:38
And all of a sudden, my costs of running my healthcare platform are affected by someone else. So there are tons of challenges here with the actual technology itself. And these are the things that kind of in the accelerator we're tackling and that a lot of people really are tackling. So we need more projects to tackle developer experience to allow for potentially people to develop in older languages or more traditional and popular languages, whether it's Python, JavaScript, Go, etc.

37:07
And their folks are actually tackling this. We need it to be more usable from our experience. I shouldn't have to explain to my father what a wallet is and have him download a wallet and remember a private key. If we've created this concept of digital identities and digital assets, it should be seamless for us to use. And we're very far from that right now. But there are, again, there are people that have been working on this within the MPC space, within the account abstraction space, to really make this a much more usable technology.

37:36
And then from a scalability and interoperability space, there's a ton of folks that have been really deep diving and tackling these technological challenges in a combined manner, enable a lot of use cases and make it a much more viable technology. A few other reasons that the technology isn't everywhere is actually, even if we take a look at the most popular chain

that we have, which is the Bitcoin blockchain, if we want this Bitcoin blockchain to be used for everyday transactions and I'm not saying it should. In fact, I think one of the most widespread uses that we're seeing right now is in payments that use stablecoins and stablecoins that basically just represent like a US dollar and there's tremendous use cases there around if you're in an emerging market or somewhere that has challenges in its own financial infrastructure, what do you do? How do you get paid? How do you store money? So actually being able to have access to the US dollar is really valuable but one of the values that fundamental aspects of blockchain technology is that everything is transparent. Everyone can see and everyone can validate that these transactions have gone through and they're accurate. But that's also a downside. If I'm a business, I don't want everyone to know exactly who I'm paying, how often and how much. Right? Not to mention that you can undercut me. You can significantly harm my business by knowing exactly what payments I'm making or not making and to whom.

39:00
So transparency is both a boon as well as a huge risk. And this is being tackled in a number of different ways. So we had tumblers that were invented that allow for people to take multiple transactions, tumble them together and have them come out the other side and that kind of hides who's doing what. Tornado cash was famously one of those that the US government decided to basically ban completely because it could be used for illicit purposes. But also we have folks that are now making like permission KYC compliant tumblers and actually one of our teams is working on that. But there's a class of technology within cryptography called zero knowledge. That's been really exciting and has really come to the forefront here. And what zero knowledge does is that it enables one party to prove that it's done something without giving all of the details that has done it. So I could potentially prove that I've made a payment and that you've received a payment without necessarily showing how much that payment was or any other details around that payment or even that I sent the payment to you. Right. And that's where zero knowledge comes in and where I was saying the Bitcoin and Ethereum math is not that complicated. That's not true for ZK. It is very complicated for ZK.

But zero knowledge cryptography has actually also been around for decades at this point, long before blockchain. came around and it was thought that it would have very few applications and now it has a tremendous number of applications. But this ability to show and to prove that you've done something without giving the details of what that is has proven really valuable within the blockchain space and people have been working on making sure that that's actually performant and that helps solve a lot of the privacy challenges. It also helps solve a lot of the scalability challenges because you're able to potentially do a whole bunch of computations locally and you're able to kind of put this proof on a blockchain, which means that instead of having to put a ton more information on the blockchain, you could just put the proof and instead of having multiple people have to simultaneously validate what you've done, that proof is there and they can always go and validate that you've performed a specific transaction or process something appropriately and also makes things much more performant and scalable aspects again that there's there's a lot of frictions and challenges in blockchain becoming popular for everyday use but these are each being tackled one by one by one. I've said all of these things about how crappy the current state of blockchain is. Again the promise is tremendous and we do see quite a number of use cases that are really viable now. The best proof of product market fit is when you see thousands upon thousands to millions of transactions happening even though the technology is really challenging to use and to build on, especially in the payment space, especially with stablecoin payments, but as well as supply chain or private blockchains that are being used within the energy space, within the banking space for shared coordination. And from an investor perspective, I think of it kind of like investing or supporting computing in the 90s, right? It was very early.

42:18
Not only was it early, there were also a lot of scams. We had the bubble that popped and there was a lot of uncertainty as to whether really we would be using computers on a day-to-day basis and the internet more so on a day-to-day basis in our everyday lives. And that's obviously, you know, completely transformed how we live our lives. I feel the same about blockchain technology. The technology itself is very early, challenging to use, challenging to run, challenging to build on.

42:48
But as each of these challenges and frictions are overcome, it enables new use cases and will become a greater fabric of the world that we live in.

MARKUS FEDERLE
Tell us a little bit about the efforts of the industry to overcome these issues. Network speed, of course, is one of the key issues here. And I think we've all heard that the industry is working on various scaling solutions or layer twos. What can you tell us about that?

GIL ROSEN
If we think about the blockchains ability to maintain itself as a decentralized platform, it's really because you have thousands of people redundantly doing the same thing, and they have to agree on consensus that the updated transactions and state and programs that have been executed have been done so correctly, and that kind of takes time. These are being solved in a number of different ways, some of which are basically saying, so if we think about in the Bitcoin scenario, one of the first layer 2s, was this lightning network where they basically said, okay, well, you have a number of people that are gonna be making transactions on a regular basis. We know that Bitcoin itself is stable and trusted, but it's slow and it's slow on purpose because that's part of the consensus mechanism. And you wanna make sure that all parties agree and that when you add transactions to a block or you add a block to the blockchain itself, it's one that has been kind of properly validated and finalized. So what they did is they said, well, let's allow a number of people to transact with each other multiple times very quickly and very cheaply. And then we'll just take the sum of those transactions and throw all of those on the blockchain at the same time. And that's kind of a very simplistic view of what a layer 2 is. A layer 2 is we're going to create this second blockchain that interacts with the first blockchain and actually handles a whole bunch of transactions in a much more performant way and a much more low cost way. And that's generally called layer 2 roll up, so to speak. And there are a lot of advantages of layer 2s. One of the challenges I spoke about earlier was that all of a sudden my cost of infrastructure is highly tied to your cost of infrastructure, someone else's cost of

infrastructure. And if they're using the network, then it significantly increases prices. It's like if we're all on Amazon, and then a bank is using their transactions and a whole bunch of people are selling and Amazon servers get really busy, all of a sudden, me running my little website, my cost skyrockets.

45:14
So layer 2s actually allow you to mitigate some of that as well, and sometimes it's actually done on layer 3s as well. But one of our projects, for instance, Caldera, has done custom layer 2 rollups. And what does that mean? That means that every project could potentially have their own little layer 2, that only their ecosystem is affected by the cost. And they can have their own miners and their own validators, et cetera. And they can determine all of the parameters of their specific layer 2. They're like mini blockchain that runs at a more performant level. And that then writes back to the main blockchain. So that's kind of one aspect, it's custom layer2s. Or the more traditional layer twos that we see, whether it's, and again, you have like zk based, zero knowledge based layer 2s, you have optimistic layer twos, optimism and arbitrum or optimistic ones. Basically an optimistic layer two is saying, well, we're gonna have a bunch of nodes that run things very quickly. And at a later date, we're gonna have people like, finalize and validate the actual transactions themselves. So you assume everything is true, you run as if it's all great actors, and then if at a later date the people around you find that performed maliciously, then you're severely slashed and penalized and punished, and that's kind of the optimistic way. Then there's zero knowledge layer 2s, which is you have a whole bunch of people kind of running and processing these transactions in the background on their own. They create a proof other people can validate that proof is accurate.

So layer 1 is basically that's the blockchain itself and that's the main blockchain that everyone agrees is trusted, has huge network effects, is operating a certain cost structure. Layer 2s allow for scaling both from a performance and a low cost perspective, all of these operations. Layer 3s allow for additional privacy and security components or kind of custom blockchains at times. And then there's also this concept of layer zero, which is if you want interoperable blockchains that are kind of these more custom blockchains that are able to run independently, but to be interoperable to leverage the same model for security, to be able to exchange assets between each other, for instance, got Polkadot and Cosmos for two examples of kind of layer 0 blockchains. We have that as well. And really, layer 0s were brought from this concept of, well, we want to have a lot of blockchains potentially, but we want them to operate with each other well, and to be able to mitigate the risk of fraud or of losing transactions between these blockchains. So we'll have like common layer of which these chains are built on.

MARKUS FEDERLE
We have spoken about the digital ledger concept and of course, about Bitcoin and storing other information on the blockchain. We've also spoken about smart contacts, but talk to us a little bit about the concept of digital assets in general. How broad is this term and what can actually be included here?

GIL ROSEN

So now that we've created this kind of shared database and the shared digital ledger, what it's storing is again, these two things. It's storing this concept of a wallet and that wallet represents an individual and their ownership of something. And it's storing transaction.

48:37
But in having this shared digital database, these wallets or these addresses don't just have to represent people. They can also represent things, right? So we can have this database that stores things in ownership of things. So it can store ownership of a specific asset, such as a Bitcoin or a US dollar equivalent, or a health record, or a security, or a bushel of wheat or a commodity. And now all of a sudden this concept of ownership has shifted. In the physical world, again, you can prove ownership because you physically own something. In the digital world, you've never been able to actually own anything. You've never been able to show that you uniquely own anything because we don't have this public place to show that Marcus owns X, Y, or Z. Marcus owns this wonderful image of an ape with bored eyes or this wonderful rocket that's going to the moon.

49:35
But this idea of shared ownership is incredibly novel and incredibly new, because not only can we show that we have ownership of digital objects and digital assets, we can have ownership of digital representations of physical assets themselves. And we've seen this again with Georgia, that put their land registry on the blockchain. We've seen this with the number of companies that are building applications in the supply chain space to show, well, who has custody of this thing.

50:04
We've seen it actually with exchanges that allow for you to own tokens and trade tokens and show like, okay, now I actually own this thing. And even this concept of making financial transactions and self-custody in the first place, we've never been able to own our own money. It's always been held by banks for us, unless we had cash. So digital asset ownership is really valuable. And one other kind of caveat there, dovetail there is even identity.

50:33
We don't actually own our own identities. So if we think about it, like in the real world, we have passports, we have IDs, so security cards, national insurance numbers, and that kind of defines who you are. But in the digital world, your identity is managed by, you know, dozens of third parties, whether it's my Apple ID, my Gmail account, my Instagram account, my login for my bank record, my login for my health record. So I've got dozens of these different identities that I don't control or manage in any way or form. And there's no way for me to limit who knows what about me. And again, being able to have a shared database where it's cryptographically safe and I can permission who has access to what allows for me to have ownership of my identity and there's this concept of SBTs or soul bound tokens that allow for me to find my own identity and control my own identity and use that identity within applications. And that's really, really powerful. Interesting segue here, there's obviously a lot of talk right now about artificial intelligence. And I think it's telling that the same founder, who's the CEO of OpenAI, Sam Altman, which now everyone's scared of AI taking over the world and being indistinguishable for humans, he's actually built another company called WorldCoin. And WorldCoin is a physical device that's gone around and scanned people's

irises, and that’s how it stores their biometric information. It just stores, again, this cryptographic hash that's representative of them to show proof of humans. Right, so now we're able to use this technology to store a specific identity and proof of that identity on a blockchain to allow us in the future state potentially to be able to show that actually this is not a human. Like what's fake news and what's real?

52:28
How do we know it's real? In the world of the internet, anyone can publish anything. And we have no idea if a video, a song, or a person is real and where it's coming from. And having these NFTs or soul-bound tokens that represent us, that can represent objects themselves, images, video, audio, that you can cryptographically prove and trace lineage of, any alterations to, can help give us back this confidence in the world around us.

MARKUS FEDERLE
Yeah, and I think also this notion of owning your own data, you know, in a world where data protection becomes more and more important, where you basically interact online, and you store bits and pieces of your data all over the world, not knowing who owns it, who has it and not being able to control it. To me, that's a very big issue.

GIL ROSEN
You're completely correct. And that's another exciting thing that zero knowledge allows you to do, which is that it allows you to share things without sharing everything about those things. And a great example of that would be personal information, biometric information, credit information. So right now, if I want to apply to get a home loan, I need to give out a whole bunch of history. And that's going to go to banks and sit in all these banking systems. And now I need to trust that these banking systems will maintain my private information indefinitely in a safe and compliant manner. And we've got GDPR that's come out to kind of hopefully try to mitigate these things, but really it's just asking other people to be good actors and more importantly to not be incompetent. Whereas in the blockchain world, you could potentially prove that you have X, Y, and Z assets. You can prove that you have ABC income and have had that income over the years and you can prove all of these things and share that information and someone can give you a loan based on or not give you a loan based on the information without them needing to necessarily all of your data on their servers. It can always sit within your own servers or cryptographically sit somewhere that's privacy preserving on a blockchain.

MARKUS FEDERLE
Gil, I could really do this all day with you. I'm afraid we're out of time for this episode of the Tholus Investor podcast. I think we have to bring you back another time to the show. For now, I would like to thank my guest, Gil Rosen, and our team at Tholus Capital for their work on this episode.

54:53
Thank you for listening and subscribing. Please stay tuned for more exciting episodes of the Tholus Capital Web3 Investor Podcast coming your way soon.