

00:16

Hello and welcome to a new BFR podcast episode, Bitcoin Fiat Rock and Roll that explores the intersection of traditional finance and blockchain and helps you to understand where digital money and digital assets go. And today with again, a very interesting episode on how public blockchains could be used in traditional finance and also which problems public blockchains might bring as an underlying infrastructure to

00:44

represent ultimately money and assets in real world economics and the real world, not only in crypto, let's say, on a completely new infrastructure, which is public permissionless blockchain. So there's lots of talking, obviously, in the industry around the adoption of public permissionless blockchains. And today I've brought two very, very interesting speakers that wrote a extremely interesting paper that I think has not yet gotten enough attention. So with me today in the episode is Wiki.

01:13

and Michael Maurer. Hi, both. Hello. Good to be on this podcast. Thank you for inviting us. Thanks, Wiki. And Wiki, maybe we start with you and a quick overview in a few minutes on what you do at Kinexis at JPMong. So you're global head of insights at Kinexis. What is that? That's an interesting title. Well, I would say I do most of the really fun and interesting work. That's probably the cool thing about having a nice title.

01:42

So some examples would really be like this research work that we've been doing with MIT. This is actually the third report that we have published together. So we have been collaborating for a number of years. We look at things like programmability, we look at deposit tokens, and now we are looking at use of public blockchain. What are some of the issues that we face and how do we resolve them?

02:03

So that's one big part of what I do in terms of just doing very interesting research work with the industry. Another area is really in terms of a collaboration on industry projects. So we are involved in a number of industry projects, a number of like central bank projects over the various years. So there was a time where central banks were very engaged on central bank digital currencies at Connexus and JP Morgan. We were one of the first to be looking at this space of

02:29

digital currency. So we were one of the banks that have always participated with a number of central banks on this particular topic of digital currencies. So I would say those are probably the two big areas. We try to look at where the future is heading and to do that, we get involved in research, we involve in prototyping, and then really look at how we can build for the future. Yeah. So not necessarily directly in the business responsible for bringing in cash, but rather on the research side, that's a very...

02:56

sweet spot, would say, even in a large bank. Yes, yes, yes. Which is why I say I do the really interesting stuff. I get to do the fun stuff while my colleagues do the hard work of bringing in the revenues. No, but eventually you will also, based on the research that you

do, bring in the revenues in the future, And Michael Maurer, I I explained it deliberately or not explained it pronounced it deliberately, but German here, German ancestry likely.

03:23

Michael, you are a research engineer at the MIT Digital Currency Initiative. Have you also been participating in all of this research reports that Wiki mentioned or what's your area of expertise at the MIT? Yes, yes. Nice to meet you all. I'm Michael. My name sounds a lot better when you say it, man. Well, I gotta say I'm an engineer at the MIT Digital Currency Initiative, which is part of the MIT Media Lab. And we do all sorts of research sort of in the domain of payments and digital currencies and sort of decentralization.

03:49

And yes, we can I have worked together now on two papers. I was not not on the first one. Usually I work primarily on database problems, know, performance payment systems, but you know, also working quite a bit more recently on the challenges of decentralization and how we can bring more and more assets onto decentralized platforms. Yeah, that's that's me. let me start with the big picture why I wanted to invite you here to this episode, because programmable

04:17

Smart contract blockchains have been around for quite a long time now, right? For quite a decade. And we're now seeing that financial institutions increasingly not only experiment with private permissioned blockchains to issue tokenized deposits, but also public, sometimes permissionless infrastructure, right? Obviously there's a strong adoption or at least an aspiration or imagination and an expectation.

04:43

to also use stablecoins and traditional finance and traditional payments, which are natively and naturally always issued on public permissionless infrastructures. And obviously also lots of banks, also asset managers or asset issuers look into tokenized assets and tokenized securities that are all then on-chain settled. And clearly also public infrastructure and public networks have the big benefit that they are public and in the sense that different players can actually operate with each other on it and allow really

05:13

atomic settlement and composable transactions. So that is happening. And I think that is also the reason why you looked into this topic and created this paper. But why did you feel that this was the right moment to write a paper specifically about the challenges that regulated financial institutions face on public blockchains? I would say that it's exactly what you have been saying. You mentioned about financial institutions and the increasing interest in wanting to use public blockchain.

05:40

We have seen that there's a lot of value in what we can do with public blockchains. You know, the ability for us to use open, interoperable infrastructure, and that really helps to support innovation across payments, tokenization, capital markets. So we see a lot of value in the use of the technology. But if you look at who have been doing some of this work, whether it's experimentation or pilots on public blockchain, you always see that same few names. You're always going to be looking at the largest institution.

06:09

And part of it is really the very high cost of compliance once we get to using public blockchain itself. So you always see the likes of like JP Morgan, BlackRock, the companies, the largest financial institutions who are willing to spend a lot more in terms of compliance costs, in terms of how we actually do development, just so that we are able to use public blockchain. So once you start looking at that, then there's always this question, why is it just the biggest financial institutions? Why?

06:37

Is it not that longer tail of financial institutions who are able to actually do things on public blockchain? And once we start looking at that, then we start to understand that the reason is really because there is still a lot of concerns in the use of public blockchain. Some of them are true, some of them are real in a sense of like there is public blockchains were just not designed for financial institutions. So very often when we want to use it, we start having to do certain work arounds and that's going to create issues in how we actually

07:07

on public blockchain. So I would say that broadly, there's a lot of interest in using public blockchain, but public blockchain will not design for financial institutions. We face certain issues using it. We end up spending a lot on our own internal compliance in terms of our operational costs as well for us to be able to use it. So there is this interest from us of like, hey, why don't we look at the problem? Why don't we list it down, look at potential solutions and then see how we can...

07:35

address it better as an ecosystem. And I think this is the fundamental tension that you can read in the paper, right? Where we come from a world where in traditional financial infrastructure, banks are really having control over the whole technology stack, right? So there's also this ASAP model from the IMF that is cited a lot nowadays. And usually the whole pillar, like the whole vertical is controlled by the bank, right? And now, especially on the infrastructure layer,

08:04

that might change, right? And where the bank or also other financial institutions don't have full control, right? So I think this is the fundamental tension that you see where banks now have to think about how that new world where the infrastructure is not controlled anymore fits into the existing compliance frameworks, but also into regulatory appetite, risk appetite, and also very concretely with regulation, right? And I think we're gonna focus on

08:33

on the different areas here within this paper as well. But one thing that I came about was basically this question, whether banks can use public blockchains or whether public blockchains need to evolve to accommodate institutions, right? Or financial institutions. Maybe to start very high level again, before we dive deep, what is your view and summarizing basically also your recommendations in the paper? Is that something that banks can become accustomed to? Or is it rather that the infrastructure actually has to change and become?

09:02

let's say financial institutions ready or TradFi ready. Well, I'm happy to start first and Michael can chime in as well. So I would say that it's definitely a mix of both. mean, banks will have to adapt. There will be certain changes in terms of our own internal processes that we'll have to make. But at the same time, there are also certain challenges that are very difficult to resolve from a banks and because we are not running the protocol. So for some of those challenges, it will be much more easier to solve it on the protocol level.

09:30

So that's where we think that, hey, it will be a lot easier and better if the protocol developers are able to solve it. And it wouldn't be just for one bank, it will be for all banks. Yeah. And I think, you know, if you had asked me this question two years ago, I would have said sort of the banks need to adapt and to move on to these changes because these are platforms that sort of exist in the wild. Now they have users that like the features that are within them and, you know, banks are sort of coming to the table and trying to enforce the rules. when we looked at this problem a little bit more closely,

09:58

We start to realize that one, there's an appetite for regulated financial assets that exist on the users of public blockchains. And right now, for banks, the hoops they have to jump through to get assets on chain are quite long and difficult to address. So we noticed that there are a couple of ways which protocol developers, which application developers can make relatively minor changes to the platform that would allow financial institutions to operate to a much greater extent on these public networks.

10:28

And also there are a handful of ways in which regulators can look at these problems and start to clarify some of the rules around how regulated financial institutions interact with public blockchains that would make it much easier for the banks to offer assets on the platform. So I think it is both. think primarily because banks and institutions are already sort of centralized entities, I think they'll carry a lot of the burden of translating their infrastructure to public blockchains.

10:55

there's still lot of room for the people who are developing for platforms like Ethereum today to address some of these problems on their end. I think probably we'll see something in the middle of the day. do you recognize already that the blockchain developer community, for example, let's focus on Ethereum, recognizes that as well and works on these problems because it is maybe recognized that

11:20

Also, the crypto community or the blockchain community has to embrace the adoption of financial institutions, which is obviously against the ethos of like decentralized Bitcoin or whatever. Right. But I think also the Ethereum, for example, ecosystem has grown up a bit to understand that if you want to scale adoption, eventually you have to bring Treadfire along. I would say it's actually not just about Treadfire. If you were to scale adoption of any infrastructure, you want the broader segment of the world to actually come on board.

11:49

So I mean, on one hand, you can't just have an infrastructure that is only end users that are transacting. Eventually, you want to bring companies on board, you want to bring corporates

on board. Eventually, if the corporates are actually on the network, they're transacting with each other, they'll start to demand things that are more institutional in nature. So that also means financial institutions will have to come in. Now, if we want to think of Ethereum as a world computer, if we want to think of it as this idea of everyone coming onto a common network,

12:17

Track 5 is going to always be a part of that. So I wouldn't even think of it as like, this is around like bringing regulated financial institutions onto public blockchains. This is really about bringing the rest of the world onto public blockchains rather than just a very specific crypto community that is only doing a very specific set of work. And I would say that when we look at the original intention of Ethereum being like a world computer, then that is really the intention of just bringing everyone on this journey together.

12:47

Yeah, makes sense. And I mean, you structure the paper around four problems that are quite interesting and quite significant. We're going to go through them. But what I liked about the paper as well, and coming back also to the ASAP model that we just talked about as well, that you really break down these problems or you describe these problems, how they could be solved also by a breakdown of what is actually constituted to

13:17

could be the reason for those problems on the blockchain. So it's not just a blockchain problem, but rather the application layer, the smart contract layer, the token standard, the blockchain network layer, the network governance and the regulation. So very distinct area to look at these problems. That's what I really liked about it. And now maybe let's start with an overview of those four problems, which is what you define front running or MEV.

13:45

censorship and transactional mission, then receipt of unsolicited tokens, and also gas fees potentially going to sanctioned entities. I think especially the latter one has been discussed in the industry quite strongly, right? This is the North Korean validator problem where eventually you have to pay gas fees to a North Korean validator, but you actually don't know about it. But that obviously is a sanction issue, right? So we're going to come to that back, but let's maybe start with

14:13

front running an MEV and many of our listeners might know what that is, but let's maybe start also at zero again, explaining what it is and actually also why it might especially be relevant for Treadfy that adopts public blockchain that goes beyond the front running and MEV processes that we know from DeFi, example, right? And cause for example, also if there's a freeze of a token that could be recognized from a transparent mempool as well, right? So maybe let's take a step back and

14:43

Let's focus first on what that is actually front running in MEV and then more concretely on how that is problematic for Treadfy players. Yeah, I can take a little bit of an overview here. So front running as we talk about it in the DeFi context is really just anytime someone knows some event that's going to happen and they insert something, maybe malicious may just be

advantageous to themselves in front of that transaction that may have a larger effect on the ecosystem.

15:10

This is, you know, this exists in all financial markets, but in the decentralized finance world, the typical way you submit transactions for, you know, to be included on the ledger is you broadcast it to a bunch of people who are building blocks, reposing blocks, or, you know, if you look at the Bitcoin world, it's miners. And then they elect to whether or not to include that transaction in a block and also where in that block it goes.

15:35

So if you're just broadcasting, for example, that you want to freeze your asset, which is something that has to be a state update on the ledger. If I am a clever miner and I have say, say tons and tons of whatever asset you're trying to freeze, I may try to basically empty my position beforehand and then process the freeze. And this is different from, I think, what financial institutions are used to typically. They get to control on their end what the order is of all transactions, especially the things that are.

16:03

is sensitive to their business processes and risks and what rules and laws they have to enforce. In this scenario where we're on a decentralized platform, it's up to a decentralized community who may or may not care about whether these rules need to be enforced in certain order. So front running with respect to traditional finance institutions is a bit of a problem. We see it a lot with DeFi trading on chain. People will try to make more money essentially off of inserting their transactions before another big market moving transaction. But now we're talking about things like

16:33

the shutdown of an asset entirely or addition to some of the sanctions list. And these are all things that can also be front run in this context. The trouble here really comes from this point that the banks, the financial institutions no longer have control over the order in which transactions get processed. And so in this paper, we talk about a couple of ways which financial institutions can sort of claw back that control. of the most, one of the ones that gets suggested to me the most and one of the ones that I think it's the most obvious to people from the blockchain world is you can just sort of run nodes and propose your own blocks.

17:02

The difficulty with that is to get a significant share of the block space on the network, you have to either stake a ton of funds or convince many, many people to accept your blocks as you propose them or have a ton of mining power, depending on what network you're on. Or create a fork. Create a fork with only those validators that don't participate in that, but then you end up the unifying ledger, obviously.

17:25

Yeah, yeah, I suppose you could create a fork and then you sort of lose all the benefits of the decentralization you wanted to achieve in the first place. So it's yeah, there are are options and they all do have have tradeoffs for sure. But yeah, looking looking at in particular at the ability for financial institutions to run their own validators and miners, you know, the limitations are really on on capital and the ability to get enough maybe in Ethereum, enough

stake to propose the amount of blocks they want to deal with on the platform. And we talked a little bit about how

17:55

They may establish relationships maybe with mining pools to get around this concern and some of the other options you may include for your asset that let you enforce these controls or allow you to enforce controls without being frontrunner to the same extent, which we can get into. But obviously if Wiki has anything else he wants to add on this point. other two proposals that you also mentioned are this deadman's switch as a solution or the fail secure deadman switch. found that quite interesting. And also fossil forks.

18:24

which are basically also encrypted mumpools. So this is now already, I would say, a completely new way to operate a blockchain. So this goes quite deep in the infrastructure layer. It's not only on the application layer or the smart contract layer. Maybe you can also give a bit of an overview of what that is or how that would work. The demand switch is actually a really interesting one. So maybe I'll just talk a bit about it.

18:51

But let's first explain the specific use case over here. actually in the previous paper where we were looking at deposit tokens, one of the things that we talking about is the need for what we call a global pause. So actually I think it's something that a lot of smart contracts implement these days. Generally this idea of possible because the moment something bad were to happen before you try to do any resolution, the first thing you do is you pause the smart contract, you stop anything else from happening and then you have the ability to resolve it.

19:20

Now just imagine from say a bank's perspective. Now if we might want to say pause a smart contract for whatever reason, but there's also a possibility that the transacting parties, they could essentially be listening on the network and the moment they see that a smart contract is going to get paused. Now before anything they're going to push, they're going to try to do something to move the tokens that they're holding. You know, they could try to offload it to someone else, maybe through the use of a defy protocol or they'll try to do a redemption.

19:50

before the the pause transaction actually gets processed. So the trouble over here is that then you you actually have this essentially the operator of the smart contract wanting to pause the smart contract and then everyone else wanting to redeem their tokens before the smart contract get paused and for them to do it on a public blockchain is really a matter of just pushing up the gas fees so high that you'll always be processed faster than everyone else. So this kind of create this asymmetry where

20:19

it is very likely that anyone with sizeable stake on the network itself, that's probably what they would want to do. And then you create this issue where the operator then loses control because you just have all of these transactions getting processed and you don't have the ability to pause your smart contract. So the idea over here with the dead man switch is essentially the idea that there's always this counter of how many transactions can be processed and then you need to process one transaction that came from the operator itself.

20:48

If that transaction is not processed, essentially everything gets paused until the operator sends another transaction again and everything else can continue. So this was one of those ideas when we were thinking through this that, hey, maybe this is one of the ways that we could implement it. Say every couple of blocks, the operator essentially sends a transaction that says everything is good, let's continue running. So it starts acting like a dead man switch because if the operator's transaction is not able to get through,

21:15

then essentially everything else is automatically paused. So that was really the idea of a dead man's switch. Now whether it's practical or not is really another question because then there's also a question of, well, you have two concerns. One is how much is it going to cost you to keep running this and is it sensible to be in a way like pushing a transaction that is mostly meaningless? That's one. And then the second is that you are not able to, well, depending on how often you actually push this heartbeat, anything before, between the heartbeat,

21:45

still get processed. I think it's one of those interesting ideas and potentially, know, institutions want to implement this really as a failsafe mechanism, but the practicality of it, it needs to be fine tuned further. Yeah, makes sense. And I can imagine that this could also still cost a lot, right? Because if then other transactions, as you said, are always before, then if that is known as well, that these heartbeat transactions need to happen,

22:13

So or illicit actors could still try to drain the pool, for example, until then the heartbeat comes. So quite costly and maybe not perfect. You also mentioned the encrypted mempools or fossil forks that basically also introduce a different mempool on a permissionless ledger. That to me sounds already quite odd because ultimately then it sounds to me already like a fork, right? You introduce some parallel mempool that might not be recognized by all of the

22:43

miners or the validators, but only by the TREAD-5 validators, doesn't that already create a fork, right? Maybe you can spend a few sentences on that one as well, those fossil forks. Yeah, yeah, happy to talk about that. I'll start with encrypted mempools a bit, and just for those who are not familiar with this concept, the idea behind encrypted mempools is all the people who are proposing blocks or building blocks have a set of transactions that they pull from. And the problem we were dealing with with front running was that

23:12

they may order transactions in a way that is unfavorable to the person who submitted the transaction. One idea that people seem to like is that you can instead say, okay, here's the pool of transactions you can pull from, but you don't actually know what the effect of this transaction will be until after this block has been accepted into the ledger. And that is sort of the idea behind encrypted mempools. A lot of the work around it has been dealing with sort of the complicated math and science that has to be done to achieve such a thing. But the general idea is that you have the ledger determine what block will be included.

23:42

accepted amongst all the validators before it is revealed what its effects are. And so the idea is that this makes it a lot harder to front run transactions like asset freezes. doesn't make it necessarily impossible. You can try to infer based on external information, but it's quite a bit more challenging to do so. So there's a lot of proposals around this that have been kicked around. We talked about some in the paper. Another thing we talk about, which you mentioned, is this forked choice inclusion list idea, or FOCAL, F-O-C-I-L.

24:11

which is really more of a censorship resistance idea within Ethereum. So if you are an institution, if you're a user that is worried about not necessarily where your transaction gets included, but whether or not it gets included in the ledger, you may be a fan of this idea, which basically has validators commit to a set of transactions that will get included in a block coming up soon. And if not, they will elect to fork off from the ledger. So this is a pretty neat idea. This has been getting some traction in the Ethereum.

24:42

world and this is not necessarily addressing this front-running problem. This is really more like if I really desperately need to get a transaction in to the ledger, then I would be happy to see it on this list itself. So I think this is good evidence that the people and developers of these ledgers are very carefully thinking about these problems. I censorship resistance has been around basically since Bitcoin rolled out as a major concern for users. And yet, definitely still today we're coming up with new and interesting ideas of how we can

25:10

can address these problems. We'll see what ends up getting accepted. forked choice inclusion lists is something that is likely to get accepted. would not be surprised at all to see some different ledgers start rolling out things like encrypted mempools as the technology gets better. But at this point, we're not clear what will happen just yet. Yeah, very interesting. And also good to hear that this is really widely discussed. I'm not that close to the developer.

25:37

community, but seems like these problems are understood and worked on. But maybe let's jump to this other problem. And I named it at the beginning as well, the receipt of unsolicited tokens. And that is quite interesting as well to me. When you think about it, when there's a SWIFT transaction today, you actually need to have a handshake, right? You need to have an RMA in order to be able to reach the other counterpart. If you cannot reach it, well, then you have to go through other settlement banks that ultimately have the RMAs with the other banks, right?

26:07

And hence here on a permissionless infrastructure, there's public addresses that can be reached by anyone. And then actually also where assets can be sent to these addresses and you cannot prevent it, right? It's like everyone can be reached and everyone can be sent illicit tokens, which can become a problem because if you then process these transactions and you actually hold them, even the fraction of a sent of a sanctioned token or sanctioned

26:37

or a flagged token that has been or a transaction that has been involved in any illicit transactions, you make yourself criminal, right? That can lead to a law enforcement against

you. So explain again, maybe, Weki, also that issue, how you look at it and whether there's an easy solution to solve that. I'm very happy to take this one. This has always been one of the pet thieves that we experience as a bank.

27:04

Let me just kind of break it down. So, receiving unsolicited tokens on public blockchain, think is a very common thing. There's often this idea of dusting, you know, very often someone is issuing, launching a new token, they will airdrop like tokens into like, like all the well-known addresses really as sort of like a marketing stunt. So it is something that has been very common. Now, the way that the Web3 companies or the general public treats it,

27:32

is very different from the way that financial institutions treat it. Now if you look at just anyone outside of financial institutions, the way they are going to treat this is this is essentially spam. This is like your spam email. You you receive a spam email, you ignore it, you bin it, you don't do anything else about it. You pretty much just ignore it and don't bother about it. Now from a financial institution perspective, the analogy that we draw is really receiving unsolicited funds in a bank account, for example.

28:00

we have processes in place that wherever that happens, we will need to return the funds. So, you know, we have to figure out where it came from. We have to then initiate a payment to send it back to the sender, original sender. Now, imagine trying to do this on public blockchain. You are going to hit a few different issues. The first thing is that... So, let's just assume what we are doing today. So, we have been transacting on base. We have a set of public addresses on base. It's well known to everyone. The thing is that...

28:30

The public address that we are using on base is actually valid on public Ethereum is valid on all Ethereum based, EVM based blockchains. So the first issue is that when we are actually monitoring for like unsolicited tokens, it's not just monitoring on the networks that we are transacting on. It's essentially monitoring on all EVM based networks, even if you are not transacting on them.

28:58

So that doesn't sound very sensible for most people, but that's what financial institutions end up doing. So that's the first thing. The second thing is once we receive unsolicited tokens, then we need to start figuring out what we need to do with it. So most of the time, if you were to say, hey, we need to transfer the token back, then essentially if you were to transfer a token back on public blockchain, that means going to the smart contract using the transfer function.

29:25

But how do you actually know that the transfer function will indeed transfer the token back? I can almost imagine playing some malicious prank where I will create a transfer function but if it came from you, rather than transferring back, that you'll do something else and then maybe even try to send tokens to a well-known sanction address, for example. So before we are able to even make a transfer back, we need to actually do an audit, a review of the smart contracts.

29:53

We need to know what the transfer function is doing before we can actually call the transfer function. So just imagine from a financial institution perspective, we need to monitor our addresses across all blockchains where the addresses are valid. We need to review the smart contracts before we are able to even initiate a transaction back. This is all the things that we actually have to do from an operational perspective. While the rest of the Web3 community, anyone outside of financial institutions, what do they do? They just ignore it.

30:22

treat it as spam and don't do anything about it. So there's a big discrepancy between how we are actually treating this and it's actually creating a lot of operational hassle for financial institutions. So right at the start when I was mentioning like cost of compliance, operational effort, this is really one of the best example where for financial institutions to actually transact on public blockchain, these are things that they actually have to worry about. But in most cases, they are probably inconsequential.

30:51

in broader scheme of things. Then there were, as you say, dusting happened, where very, very fractional amounts of these coins or these tokens were sent to random addresses, sometimes even like public figures.

31:18

then it was clear that the celebrity is now part of an illicit transaction because it was mixed and run through a mixer. So that is one problem. But then the other one is really also when there's a new token created, which has via the token smart contract certain functions that you would need to call in order to return it, then you don't actually know what's happening. So you need to audit the code ultimately, which obviously creates a huge operational burden. Very interesting. So, and you say basically there is not yet a clear

31:48

solution to that problem. Every bank acts or every player acts differently on it to actually manage that risk. Yeah, so this is really one of the examples where if you are able to solve it on an ecosystem level, it's going to be really good for the industry. It's going to help all the financial institutions looking to actually transact on public blockchains. Coming back again to the Mempool that we have focused on also,

32:15

in the front running and the MEV transaction. There's also something that we named or mentioned in the beginning, the censorship or transactional mission by basically introducing private mempools. I think this is also what I had in mind when I said, doesn't that create already a fork in the sense of restricting access to mempools on public permissionless infrastructures?

32:40

as the name says already, public permissionless infrastructures include a completely transparent, but also public mempool where everyone can push transactions into. And I think to solve this problem, where you could also censor certain transactions that you don't want to process as an issuer, where the issuer eventually also needs to have more control other than a simple whitelist approach.

33:08

You say that there could actually also be private mempools. And what I found super interesting is that apparently already a significant share of the Ethereum activity is run on private order flows in private mempools. So maybe you can briefly also explain that issue and then how that private mempool solution would work. Yeah, happy to get into that. Just clear for one thing on the mempool and that's sort of how that relates to the ledger. You actually see...

33:37

You know, by and large, most miners, most validators, most block builders do have some sort of a private mempool. There's some set of transactions which they have, which may be their own transactions, which may be transactions they don't want to share with other nodes, for example, that they just keep to themselves. And they may then include those in blocks that they propose for the ledger. So the mempool is not necessarily a shared thing, although in reality, and a lot of the implementations of the software for these ledgers,

34:04

There's a gossip and so people tend to have a relatively common shared view of what's in the mempool I think this is especially true in Bitcoin where the gossip protocols is pretty strong, but in aetherium and then a lot of the other platforms You see fairly large, you know builders It's listing transactions directly from people who want to get them included and not gossiping them around around the network So they have this sort of private list of transactions that they can choose from

34:31

They do this because their entire goal is to make money out of this. So they may not want to share a transaction that is particularly profitable to them. The client could always send their transaction to multiple builders, sets of builders, and that would get a guarantee that their transaction is included faster. But if they had, for whatever reason, established a relationship with a company like Nethermind, for example, who builds a lot of blocks, then they may only, for example, send their transactions to them.

35:01

a very private sort of transaction is not shared with the rest of ecosystem before they're published. So we bring this up as one option because this is something that is pretty familiar to banks already. can establish relationships with, know, banks establish relationships with cloud service providers, for example. This is a very similar situation in which, you know, a bank could get into a deal with a block builder and say, hey, you know, if you get a transaction from me, I expect to be included in your

35:27

one of your next say five blocks and I expect you to process this transaction before any other related transactions. And these could just be based on traditional contract law. Maybe there's some incentive for the block builder that no longer does the block builder have to just take the profits from the blocks they propose. They may also get some payout from the institution they're collaborating with. And so how this relates to centralization, decentralization. I think the hit on this idea is generally that you are now removing

35:55

the ability of smaller miners, smaller block builders or proposers to have these transactions in their set when they build a block. And I think that it does hurt decentralization to some extent. think in some of the ecosystems, this would be more of a concern than others. I think in platforms like Ethereum and a lot of the Ethereum L2s where there is already a pretty strong degree of centralization of certain assets, I think this is less of a concern. I mean, you already see things like USDT and USDC, which are

36:24

stable coins controlled by Tether and Circle respectively. And at the end of the day, this is an asset that while it's on a decentralized platform is a centralized thing. If banks start issuing their assets on public ledgers as well, you're dealing with the bank's asset. You're not necessarily dealing with a decentralized conglomerate of banks just because you're on this decentralized ledger. So I think we're already sort of pushing towards centralization on that regard anyway. think that the users of

36:52

of tools like deposit tokens will already be accepting of that. I think this is actually a pretty nice happy middle ground in which you have the transactions existing on a public ledger already. They're intermingled with the rest of this decentralized network and the things that have to be centralized because of the nature do get centralized. They get sent through a limited set of block builders, for example. It does introduce a scenario where you may have banks picking favorites amongst the set of people who build blocks, but...

37:20

That is something we already see today in traditional finance. I think it's not a major concern for these networks themselves. least that's how I see it. think many people who are much more strongly in decentralization may disagree with me there. think dealing with centralized assets, you're going to have some points of centralization anyway, so might as well accept it. So maybe less critical problem to be solved or?

37:47

solve for because there's already some sort of centralization and that we see. This is the fourth problem that you also outline, which is very, very interesting as well, obviously. think quite, or let's say more publicly discussed already over the last years, is this sanctions issue and the North Korean validator problem. Is that possible that regulated financial institutions

38:13

and can pay gas fees or are supposed to pay gas fees to eventually sanctioned entities. If a bank ultimately cannot control who receives the gas fee associated with that transaction, how can it then also guarantee the sanction compliance? I think one of the solutions that was proposed is the Convase opcode, or at least described. But that is on the application layer.

38:43

does that stop working or what does it actually do to solve this issue? Yeah, yeah. So this is I think a very interesting question. I think this one and the one around receipt of unsolicited tokens do start to touch on where regulatory clarity may play a bigger role on these platforms. But to answer your question, we talk about some ways in which you may, as a financial institution, try to reduce your exposure to sanctioned entities. So basically try to reduce the

39:11

likely that you pay out some fees to be on the North Korean miner, as you said. One idea we pitched was you can use one of the opcodes that's available to you in the Ethereum virtual machine, which is what processes all the smart contracts on Ethereum, is this Coinbase opcode, which miners use to specify who should get the reward from the block. So all of the fees that are paid out beyond the fee that gets burnt goes to whoever's Coinbase opcode is specified.

39:39

One way you could approach this problem, and this is not really the best way to do this, but I could say, OK, in my contract, I specify if the Coinbase opcode matches one of these 10,000 addresses, then transaction has to fail immediately. That is sometimes convenient if you have a list of addresses that you know are sanctioned that you know you cannot interact with. But the challenge is that it's effectively free to generate a new address. Like if I am a clever, you know,

40:08

person in North Korea trying to receive Ethereum fees, I'll just roll another address and move those funds from my original account to a new account where I can then offload it through whatever exchange will take my funds. So it doesn't really get to the core of the problem, but it is a way for financial institutions to at least try to address this issue. This is one where we had a particularly hard time identifying ways that

40:35

financial institutions can go in and today prevent this issue from happening. I think the way that, at least to me, the way that this should be addressed, this could be addressed most effectively, is if there's a little bit more clarity on what institutions have to do when they're in a situation like this. What precautions they have to take to not be in the situation and also what they should do if they end up in the situation. Because right now, the sanctions are obviously a strict liability.

41:04

if a bank interacts with a sanctioned entity, is very, very bad for them. very costly. It cost a lot in fees and legal pain. So a little bit more clarity here I think helps a lot. There's only so much that you can do on the application layer to get around this. given that we're operating in a decentralized system, by nature, you don't necessarily know who you're interacting with.

41:30

on any given transaction. That's one of the reasons people like to use this platform. One of the things that makes it easier to innovate on is the fact that anyone can interact with it. But that means now we need some way to understand what to do if you end up a situation interacting with someone you do not want to be interacting with. So that would be a prime example of what could be done in the application layer, although not solving the issue completely, right? And I think also what you propose is like

41:58

safe harbor provisions for those institutions that have taken reasonable steps to avoid those sanctions interactions on the application layer, inevitably encounter some residual exposure

and cannot do anything about it. the regulator should also, I think based on your proposal, recognize that issue, see whether you took some reasonable steps to avoid those, but ultimately you cannot prevent it. And I think there's this

42:28

Proposer-builder separation that goes even deeper, right? That goes rather into the settlement infrastructure and not only on the application layer. Can you also briefly explain how that would look like? Yeah. So, proposer-builder separation is essentially the idea that Ethereum is using now, where the builder of a block is not necessarily the person who proposes it to be included in the ledger. most of the transactions that are on-chain today are being

42:58

included in blocks that are built by a small set of very large block building companies. The idea that we were sort of kicking around there is if financial institutions are interacting with block builders that they know and they can trust, then maybe there is a way for them to build blocks in such a way that fees only get paid out to the block builder from those particular transactions. The challenge there is the block builders have to compel the people who are proposing the blocks to actually use them.

43:25

So this may hurt their ability to incentivize that. But that was another way which we pitched that allows the financial institutions to interact only with the entities that they know and that they can trust that is sort of that is related to how Ethereum acts today. But it doesn't really resolve all of the issues. If now this builder interacts with someone who's a sanction entity, where does sort of that chain stop? Is the financial institution responsible for that interaction? Really, really hard to say without.

43:55

bit more clarity. very interesting. And now we dived quite deep over the last minutes on those four specific problems, So MEV, unsolicited token censorship on the mempool side and also sanctions. mean, other problems that you also described in the paper, and then I think those are also more known, let's say in the wider community, are all also attributable to a

44:23

public permission is ledger. So for example, the risk of a fork duplicating the balance in a token smart contract, or for example, Circle as a stable condition also had to specify in the Ethereum fork or the Ethereum merge ultimately that only the smart contract on the new proof of stake chain was supported and thereby ultimately also interfering the democratic decentralized process of choosing the right blockchain, which obviously the community should do.

44:52

So here the risk of forking means basically duplicating the amount of outstanding stablecoins or also tokenized deposits or deposit tokens that would be issued on or ultimately, of course, also securities that would be issued on public versions ledgers. So that is a problem that you also described. Settlement finality, think, is something that is quite well understood or at least discussed, right? Because blockchains usually only have probabilistic finality, at least layer ones.

45:21

with permissionless validator or validation or mining processes. So they have probabilistic finalities with decentralized consensus mechanisms that really cannot provide legal finality that you would usually require for transactional settlements. Like we know, for example, from RTGS systems or other clearing systems, also ultimately banks providing nostril accounts, they are the ones who say that is final now, right?

45:48

and then send a credit notification or ultimately an account statement at the next day. That doesn't exist. And then the other one is privacy. Clearly, Mempool is very visible and also all the transactions are visible. So not only the validators, but ultimately everyone through a blockchain explorer can see what happens. And yeah, you need solutions like zero knowledge proofs. think we've discussed this quite extensively also in this podcast, obviously something that is known in the industry. However, it's still

46:18

very much computational, has lots of computational effort and lots of compute needs to go into that. Zero knowledge pools have been now established to some extent in layer twos, like at ZK rollups, but it's still quite costly and in its early, let's say state, I would say in the adoption of also traditional financial players. And then the last one, just to mention again, is quantum resistance, where you say ultimately the...

46:46

cryptography for signing transactions and the relationship between the private and public keys could be hacked by quantum computers or could be interfered with by quantum computers. And to solve it, the ledgers really require a new signing and cryptographic algorithm, which requires coordinated hard fork ultimately. So the whole community to agree that that infrastructure has to be upgraded. also quite hard problems to solve for, right? But I think

47:13

more or better understood. And all of these questions seem really to lead to the same conclusion. You can't solve everything on the application layer, right? But rather maybe also on the infrastructure layer. And also the question why banks cannot simply build sophisticated compliance and smart contract infrastructure around public chains where the underlying protocol is untouched, right? That might not suffice, right?

47:42

So how much decentralizations do institutions actually need? think that is also a quite interesting question that comes up. Is that something which obviously the public blockchain industry proposes as the new way to organize financial markets and stuff, is that actually realistic? There are quite a number of questions that you mentioned. So I'm going to pick and choose a few and then just respond to them. I mean, the first question around like why can't banks just build?

48:12

compliance, risk management kind of tools to manage the risk without touching the underlying protocol. I would say that we definitely can. mean, the view of like financial institutions like us having transacted on public blockchain means that we have managed to

cross the line, that there were certain risks that we are able to manage it sufficiently, that we feel comfortable enough with transacting on public blockchains. And also really the point that, I mean, the regulators have not stopped financial institutions from

48:42

transacting on public blockchains means that at some point in time they have probably looked at you know what some of these institutions are doing and they are sufficiently comfortable with it. I mean that that would be my view. But then it goes back to my initial point which is this is really not just about the biggest institution. If you are willing to spend enough, if you are willing to put like you know enough resources, enough people

49:09

to manage these risks, I think you can always get yourself comfortable. But would you want to be spending millions on compliance? And then what does it mean for like your smaller banks if they are only like, you know, like \$100 million a year on their IT budget, would they want to spend like, I don't know, three, five, \$10 million just on that compliance so that they can transact on public blockchain? So as long as we are looking at compliance costs in the millions,

49:38

then you are restricting the type of institutions that are able to transact on public blockchain. So the point is really not about whether we are able to cross the line. The point is whether the broader set of financial institutions, are we able to cross the line at a reasonable cost at a place where we are able to feel comfortable with using public blockchains. So that's one. The second one actually relates to the first point as well. The point around like, you know, public permission networks.

50:07

So I think we are starting to see a lot more of like public permission networks. They are not just purely like truly public permissionless network because we start to see that with the addition of some of this permissioning, with the addition of certain kind of like safeguards on the protocol layer, you are able to make it a lot easier for financial institutions to transact, which is why I do feel like we are starting to see a lot more of such networks coming up.

50:36

We're also seeing like layer 2s coming up and some of these networks because of the way that they are developed, they are able to make it easier for financial institutions to feel comfortable transacting with them. But do we have a good solution as yet? I don't think so. I think that even with some of these public permission networks, they probably solve the problems better than say public Ethereum. But would any financial institution be able to tomorrow use them immediately?

51:05

I we are still far from it. So I always like to use the analogy of like cloud services. 10 years ago when we first had cloud services, there was always that number, small number of larger banks that went on first. Then in the whole process of them using it, the cloud services provider learned from it as well. They make it easier for other banks to be able to use it. They often filled up like some of these questionnaire. So they have pre-filled up questionnaires to provide to the banks.

51:33

so that they have like information that they can provide to the regulators almost directly. I think we are starting to reach that kind of phase where we are going to see a lot more of a public permission network that are designed for financial institutions that are up and coming. But of course, it goes back to the question of what is the right kind of architecture? Does permissioning actually results in losing some of the benefits that we see from public blockchains? Does that having an operator essentially

52:02

means moving away from pure decentralization? Is that something that we are comfortable with? I do feel like these are questions that we need to really understand as an industry and figure out, you know, there are all of these different trade-offs. What is the right combination of trade-off that we should eventually arrive at? And that's something that we have been very interested in and really actively working with other people on as well. And we see two different approaches, I would say, in the permissioned

52:30

public networks, as you mentioned. So first of all, layer ones that have a permission validator group, let's say we see Temple from Stripe and Bridge, for example, and others, but also Arc from Circle that also start now with a restricted pool of validators, right? Eventually they also say they want to open up and become permissionless, but that is one solution. So new layer ones that eventually also are built.

52:55

maybe around the problems that you also define. Let's see how far they get in solving those issues. But then also layer 2s that ultimately have a centralized sequencer, right? Where, for example, a centralized entity runs the access, runs the nodes, or actually only one sequencer node that restricts ultimately access, but then also ensures

53:19

settlement finality ensures that the mempool is clean and basically controls the access to that network to not only from a, or actually not from a wallet perspective, but more on the transaction processing perspective, right? Quite two interesting approaches in there, especially I think layer twos seem to be now also entering traditional financial markets with some of the entities now looking into that. Whereas others try to build a new layer one that obviously also has to be adopted.

53:48

So interesting approaches, but when you think about like the future, and it's maybe looking at the time come to slowly to an end of the episode, what would a perfect solution look like? Is there a perfect solution from your perspective or is it still in the making that needs to happen from within the industry or actually also maybe from within TREADFY coming together and designing an operational ledger that works for them.

54:18

Well, it's quite funny you're asking this because right after this podcast recording, Michael and I are actually having a meeting to talk about this. This is something that has been really interesting for us. Like what I was just mentioning, ultimately we see that there are trade-offs. What is that optimum set of trade-offs that people are willing to live with? And I think it

has to come from the broader industry as well. mean, it's not just about what JP Morgan thinks about this. It's not about what MIT thinks about this.

54:45

it is really around the other financial institutions. Are there certain red lines that you just cannot cross? Are there certain requirements that are so critical that you cannot live without it? And what we are trying to do is really to get this understanding across financial institutions and that will then help us to understand, if you put all of these requirements together, you kind of draw the line at these are certain things that we always must have. These are certain boundaries that we can never cross.

55:13

you then narrow it down to a much smaller set and that helps us to move towards like what an ideal public blockchain for institutions look like. Maybe public even isn't even the right word to use. Maybe I will reframe it even more. What does an ideal open blockchain for institutions look like? That is a problem that we are trying to understand. That's a problem that Michael and I are working very actively on. And that's something that we do hope to bring in even more people to

55:42

to just talk to us, work on this particular aspect. And then as the industry, as the ecosystem, we have the ability to then define like, this is what we think an ideal open public blockchain looks like. This is how we could potentially work with protocol developers, potentially even amongst the financial institutions to really come together and work towards this ideal state. And this is a very interesting question. think the underlying point is like, if we think that people, customers of banks, financial institutions want to interact,

56:13

with these decentralized protocols. We want to understand what it is that really is sort of the draw for users to these platforms. I think there's many, many reasons why someone might use a decentralized platform. For large institutions, it seems like they still want to have access to traditional financial assets, deposits to the bank, and they want that to be integrated into the platforms in which they're doing sort of their other business, whether it be Ethereum or Bitcoin or otherwise. And I think what we want to understand is

56:40

as we sort of push on the networks to change a bit, what does that take away from its utility to the customer? I mean, at the end of the day, think the banks, they want to be where their clients want them to be. I'm saying that as someone who's never worked in a bank, but that seems to be pretty obvious based on what I'm observing and how banks interact with public stands. And so, we're trying to very seriously look at this question of what is it that draws people to these platforms?

57:08

What are the new things that people are developing on these platforms that couldn't exist in the current financial ecosystem? And do the changes we're advocating here hurt the ability to do that? Sometimes it is just about understanding the trade-offs. I think as more more platforms come up, you mentioned ARK and Tempo, we haven't yet seen what will be done on those platforms and whether or not they'll attract the same sort of users as exist on Ethereum today.

57:36

I think that would be a very interesting case study in if offering these new features is something that causes these networks to boom and causes people to innovate and flourish in their development. But for now, we're trying to offer the entire ecosystem our view on what is useful to consider as a modification, but also what we, to this point, understand would detriment these systems if you were to roll these out.

58:04

And yes, we would very much like to open this question to more financial institutions and more people who are developing on these platforms. I think this is a conversation that the ecosystem will really need to have if this is going to be something that is sort of useful and then we'll take off. Maybe to wrap things up, think what the paper also mentioned is that not only the infrastructure layer should be looked at, but also from the regulatory lens, these problems should be understood and then also

58:33

clarity should be provided or at least helped to provide clarity on, for example, treating front running of financial transactions as market manipulation, how it is at the moment as well in traditional finance. And then obviously you also need to ensure that this is not done eventually by the things that we discussed. Then clarifying obligations throughout unsolicited tokens. What does that actually mean?

59:00

mean from a sanction perspective, but then also the other problem that we discussed how to deal with that. And then clarifying reasonable sanction controls, providing safe harbor for unavoidable residual exposure, what we have discussed when financial institutions actually invest into using application layer solutions and then still having that marginal risk or that residual exposure and then ensuring that

59:28

they don't necessarily get enforcement. So there's also an ask to the regulator to look into it and to cooperate, let's say. So let's see where we land. To wrap things up again, I think I've said it the third time now, final statements, basically, is the next thing that you work on? So is there something that you already know that you definitely also want to look into? I guess it's hard for me to say. think we're hoping, and the conversations that come from it, help us understand what the

59:57

the problems are that really need to be solved in the system. think understanding what these trade-offs really are and how, you know, trying to build something for an entire economy is very hard because there's so many different perspectives and just trying to consolidate some of these thoughts and perspectives down into something that is tangible will help us really know what the next next things need to be developed. Our next thing that needs to be advocated for is. So I wish I could answer that question a little bit more cleanly, but that is sort of where I stand at this point.

01:00:25

I would welcome industry adoption or an open industry conversation, Where not only the TradFi space would discuss all these things in some sort of forum, but also, for example,

developers come together and also work jointly on these problems and provide solutions. So similar, what you also said, we don't yet have the perfect solution and the perfect infrastructure, right? How would this shared ledger for financial institutions actually look like?

01:00:53

who could provide it. And I think there are a few industry initiatives that already bring lots of commercial banks, but also central banks to the table where these things could eventually also be discussed if they were open to these complex infrastructure questions and not to say, let's just build our own private blockchain and rather look into public permission or potentially permissionless infrastructure. Yeah. So this is really how we are thinking about it. I mean, when we are putting together this research,

01:01:22

When we are publishing the research, the intention is really to shed light on the problems that we are facing. Really helping people to better understand it. Some of it is around proposing solutions. The idea is really that if we can get more people looking at it together, it makes it a lot easier for us to get towards an ideal state to actually go beyond just thinking about something, but actually to actually solving it. So I would say, you know, the...

01:01:50

The next step for us is going to be around researching, it's going to be around like defining the problems, getting a view of what the ideal state looks like. The step after that would naturally be to operationalize it. Whether it's us, whether it's JP Morgan, whether it's MIT, whether it's some other parties from the industry, or perhaps all of us coming together to solve the problem. I would say that's the subsequent steps. And I do hope that we would be able to move towards that solution.

01:02:19

because it's going to create a much better world for all of us who wants to transact on open blockchains. With that, think we can close the session because we can all agree to that and I would love to see that. So guys, thanks a lot for coming and for joining this episode. It was fascinating. I really enjoyed it. Thanks for all your insights. yeah, we'll link the paper obviously and the show notes and would love to have you back at the episode and then talking about the next book. So thanks a lot both. Thank you so much.

01:02:49

Anyway, I just wanted to end with something funny, which we'll probably cut out anyway. So, know, at the start, before we started on the podcast, you asked about, you know, why the title of Head of Insights? The funny joke is that at the end of a lot of these conversations, we always get a thank you for your insights. So yeah, that's helped to explain the title that I have at Connexus. Yeah, thanks for your insights. Yeah, thanks, Memo. This was fun. Cheers, guys. Bye. Thank you. Bye.