EPISODE 1271

[INTRODUCTION]

[0:00:00.3] JM: Platforms like Ethereum have billions of dollars of market cap and large developer communities. However, it is still a challenge to build widely adopted dapps on it, because of current limitations. Blockchain proof of work transactions are typically slow and proof of stake transactions trade off decentralization to achieve high throughput. Transactions fees get expensive, especially for high network load times. Scalability is low and this creates a bad user experience.

The company Polygon, previously Matic Network solves some of these problems with their platform for Ethereum scaling and infrastructure development. Polygon combines the features of standalone blockchains, like sovereignty, scalability and flexibility with Ethereum, security, interoperability and developer experience. These features enable scalable solutions on Ethereum and support a multi-chain Ethereum ecosystem.

In this episode, we talk to Denis Ermolin, a Senior Software Engineer at Matic Network. Dennis was previously a senior software engineer at Any Mocha Brands and CEO of Moon Realm Entertainment before that.

A few announcements before we get started. One, if you like Clubhouse, subscribe to the club for Software Daily on Clubhouse. It's just Software Daily. We'll be doing some interesting clubhouse sessions within the next few weeks. Two, if you are looking for a job, we are hiring a variety of roles. We're looking for a social media manager, we're looking for a graphic designer, and we're looking for writers. If you are interested in contributing content to Software Engineering Daily, or even if you're a podcaster, and you're curious about how to get involved, we are looking for people with interesting backgrounds who can contribute to Software Engineering Daily.

Again, mostly we're looking for social media help and design help. If you're a writer, or a podcaster, we'd also love to hear from you. You can send me an email with your resume, jeff@softwareengineeringdaily.com. That's jeff@softwareengineeringdaily.com.

[INTERVIEW]

[00:02:03] JM: Denis, welcome to the show.

[00:02:05] DE: Thank you.

[00:02:06] JM: Today, we're talking about blockchains, specifically Polygon and which is previously known as the Matic Network. I'd like to start off by talking about why Ethereum is not the end all be all for building blockchain networks, for building smart contract applications. There has been a number of alternatives to Ethereum for building smart contracts and decentralized applications. Why is Ethereum not the perfect solution? Why are there alternatives to it?

[00:02:45] DE: Right now, it's quite simple. It's scalability issue. At the moment, Ethereum provides about 15 transactions per second. It's not enough to for any series mass adoption so far. Because the block space is scarce, they guess, the prices to get into the block is just growing exponentially, especially the last six months. That's why there are more and more competitors arising that provides alternative solutions to Ethereum that are cheaper and faster.

As any blockchain, there is a trilemma problem. It's a decentralization. It's a scalability and security. Ethereum mostly focuses on decentralization and security. Most of the alternatives, they are sacrificing either decentralization or security to gain the scalability. As a layer one blockchain that as a base layer blockchain, it should be secure and decentralized at first. That's why we are building Polygon to actually scale the Ethereum further, but rely on the security of Ethereum itself.

[00:04:32] JM: The networks other than Ethereum, they are often Ethereum compatible. Can you explain what Ethereum compatibility is?

[00:04:43] DE: Yeah. Ethereum is using Ethereum virtual machine, or EVM. It's a basically, execution environment for the smart contracts. Any programmer that know solidity, it's a programming language that is widely used for EVM-based smart contracts. They can just write some Turing complete code, and it will be executed in a decentralized way on EVM.

Why the competitors are EVM-comfortable, or Ethereum comfortable is because they exist in code base of some projects. It's just huge. I was working with some basically, a prediction market project. No, it's just huge. That's a lot of code. If some if the competitor want developers to make a transition from Ethereum to their solution, it has to be comfortable, because otherwise, nobody will want to redo all the work from scratch. It's years and years of work. Tens of thousands human hours of work.

That's why most of them, they provide this EVM comfortable environment, so it's easy to make a transition for existing developers. Plus, the whole Ethereum ecosystem developers, they don't have to learn another language that might be, have even more problems. Because solidity is constantly upgrading and very careful work should be done, because millions of dollars are on stake. Of course, nobody wants to try something new. Because it's expensive, it might be insecure. Not battle tested enough. Yeah. That's most of the reasons why alternatives want EVM compatibility.

[00:07:04] JM: If I write and deploy a smart contract to Ethereum, and then I write and deploy another one to an Ethereum-compatible network that is not Ethereum, can those two smart contracts communicate with each other?

[00:07:23] DE: They can't really communicate with each other in the way – within the same transaction, within the same environment, because they basically, two separated databases internally. In theory, it will be possible if for example, machine could run two blockchains at the same time. In practice, Ethereum is difficult to run. It's not an easy task for consumer grade machine to run the Ethereum node. Their high throughput alternatives, they require specialized equipment.

In the practice, it's not feasible to run, to change the same time and make them fuse together. The way two smart contracts can communicate like in quotes with each other, it's an off-chain messaging, some kind of off chain messaging protocol. Our Polygon bridge, for example. We have Ethereum chain and matic channel, matic side chain. The way you transfer the token from Ethereum to Polygon, is by locking the tokens on Ethereum side in the bridge contract. Then the bridge contract emits the special event that being picked up by our chain.

Then within the consensus, they mint tokens that were emitted on Ethereum chain. It's basically, some message being picked up by our chain. It was a bit different way from the Polygon to Ethereum, because Ethereum don't have this special modified code that can pick up the events from Polygon. The way it's done from Polygon to Ethereum, the tokens being burnt on Polygon side, and then user provides special proof to the bridge contract. Then when the breach contract checks that proof is valid, it just unlocks the necessary amount of the tokens on Ethereum chain.

This is the example how smart contracts might communicate with each other. We can pass the same way any arbitrary data between chains. It's not instantaneous. It's not within the same transaction, but it's possible. You might even perform calls on a different chain, like you're passing a whole transaction, like sign transaction between the chains, and then one of the sides can just execute the transaction within the EVM.

[00:10:27] JM: These blockchains other than Ethereum that are Ethereum-compatible, what are they sacrificing? What are they gaining in their alternative architectures?

[00:10:42] DE: Yes. The majority gains are in the scalability, in the performance, like how many transactions per second they can execute. What they sacrifice is either decentralization, or security. It's hard to tell like, what is mostly popular? I think in 2017, URS, or right now Binance chain, they mostly sacrifice in decentralization, because 20 machines are running.

If less machines are running the same code over and over, like replicating the execution process, it's easier to push the limits of the node. Some are actually have a lot of nodes, but I think they're sacrificing security. Some of them have really, really novel ways of achieving the consensus within the chain, within the network. It's not battle tested and we still don't know what are the security holes, potential holes are there. Basically, one of those. Since the scalability is the problem, they pushing the throughput and sacrificing mostly the security, I would say.

[00:12:20] JM: Got it.

[00:12:21] DE: Yeah. At the same time when you're sacrificing decentralization, is also sacrificing security at the same time, in a way. Because if less nodes in the network, it's easier to break the consensus to different kinds of attacks, like collusion of the validators, for example.

[00:12:46] JM: Got it. Just to go a little bit deeper on that, so when you talk about breaking security, or breaking decentralization, is that because there are fewer nodes that are validating the transactions?

[00:13:05] DE: Yes, correct. Yes. That's a decentralization aspect of that. Because yeah, as I said, it's easier to gain the chain if they are less nodes to be compromised, or they just can collude with each other and steal the funds, eventually. It depends on consensus. Generally, more nodes in any decentralized system, more elements in there will provide better decentralization and inherently, security. When I'm talking about security and decentralization, the connection between them, that's just a censorship resistance, and the security of the funds in general, because the security aspect is a bit different aspect. More like consensus and how stable the chain might be.

[00:14:12] JM: Okay, so let's start to talk about some of these different Ethereum-compatible blockchain networks. We've done shows on a few of them. We've done a show on Polkadot. I think I might have done a show on Cosmos. I can't quite remember. Can you just tell me, give a few examples of Ethereum-compatible networks, the trade-offs they make and maybe whether or not they have any usage, or what their use cases are?

[00:14:46] DE: For example, Tron. I think this is the most famous EVM compatible chain at the moment. Yeah, so Tron was originally a fork of Ethereum client written in Java. Right now, I'm not sure where are they in terms of development. I guess, they just continued with that. Otherwise, it might be a problem to upgrade to give the client that is maintained right now by the Ethereum community.

The Tron is running, as far as I know, it runs on the – or a proof of authority kind of network. Basically, it's something like Binance chain as well. Yeah. Here, they mostly lack of decentralization, because I don't know exactly how many validators in Tron, but it's probably less than 20. Yeah, I believe that most of the nodes, same with Binance chain is just being controlled by the Tron foundation, and is basically just side chain that run under the Tron

foundation. As long as the Tron stays trustable, as long as people trust in this chain, yes, people are fine with that.

The other EVM-comfortable chain, I mean Binance chain too is pretty much the same story as a Tron. We're trying to find something other than that, that is EVM comfortable. Phantom, I know. To be honest, I'm not sure their stats, but they're definitely sacrificing something. Because it's still it's layer one. It's a standalone chain. They definitely don't have the securing properties of Ethereum. Not even close. Any chain, like ontology, same problem. It's proof of stake system. Proof of stake systems, they tend to be faster than the proof of work systems, due to the fact that you don't have to perform the work itself. The proof of stake systems usually don't replicate smart contract execution over the whole network. Usually, proof of stakes, they have some cycle of validators. Each time, let's say, every five seconds, the network decides which node will produce the next block. This way, it can scale way beyond that proof of work networks can do, because it's just one node producing block at the same time. The rest are they just agree on the result.

Proof of authority is pretty much like proof of stake, except there is nothing at stake. It's just nodes that are producing blocks. It's even a worse system, to be honest. It's just being, trust us that we're going to produce valid blocks. That's why it's called proof of authority. Yeah, so the most harmony, also EVM-compatible, all those chains, they're mostly proof of stake. Of course, they're sacrificing either security, or decentralization. As I know, harmony have a lot of validators, as far as I know, but they use a novel consensus that has been different and we don't really know what might arise from the security standpoint.

[00:19:14] JM: All right, so we've talked through the domain a little bit. Why don't you give me a high-level explanation of what Polygon is.

[00:19:26] DE: The Polygon, let's say, there is a Polkadot with this idea of interconnected blockchains, where there is normal – what they call base chain, and there are power chains that are being connected to the base chain. Those power chains can communicate with each other in a way, like I told you on this bridge messaging, but in an optimized way.

The Polygon is something like Polkadot. Instead of base chain that is just chain on itself, or like Polkadot, we use Ethereum for that. We derive the security of Ethereum in a way that the results of execution on Polygon side is being saved on Ethereum. The final state of the whole ecosystem is being set in stone on the Ethereum side, that is way more secure than any smart contract platform out there, like magnitude is more secure and decentralized.

The problem was that all LT solutions right now that they're pulling away the users and the projects from each other from Ethereum, and the space become fragmented, like heavily fragmented. The main purpose of Polygon, first is to solve this fragmentation problem and fragmentation of liquidity, if we're talking about defi. Because the application, so the Polygon SDK allows developers to create a chain that is specific for the dapp, so they can tune speed and security purposes. Speed and security parameters that fits their application.

For example, some financial defi application probably want their users funds to be as secure as possible. They might go with ZK roll-up, for example, as a way to scale their, let's say, poly chain, like Polkadots power chains. Maybe there is some game dapp that don't want that, but they don't want to scale a lot. They might go with some easier solution, like proof of stake solution. It's very fast and very scalable chain, but at the same time, it lacks some of the security attributes of ZK roll-ups, for example.

The base chain of all the Polygon ecosystem that is being connected to Ethereum, it can pass the messages between those poly chains. This way, when locked, their liquidity between those chains and basically, we just merge all those chains within one huge space and they can interact with each other. It's not fragmented anymore. It becomes a whole.

Yeah, not to mention that now, developers can easily spin up chains and tune the security and scalability as they want to be. It's very, very easy to spin up those chains. In a way, our scalability of Polygon ecosystem is just infinite, because dapp can just spin up their own chains and we can spin up infinite amount of chains again and again. All of them being secured by the Ethereum layer and the very basic base chain. They all tied to do that.

[00:23:15] JM: Just take a step back, I want to revisit this. What are the applications that need these alternative Ethereum-compatible chains today?

[00:23:29] DE: Right now, most of it is defi dapps. For example, how they move to us months ago, or 3 billion of liquidities secured on Polygon chain right now. Demand is there. Social swap, curve, finance. They're all moving away from Ethereum, because the gas and the transaction price is just ridiculous right now. Four-digit transaction price at the moment. Mostly, it's defi applications at the moment, because it's the most popular dapps on Ethereum right now. There are more projects moving to us, some NFT projects, some games. They're all looking for cheap alternatives, because you really can't achieve anything. For any small action, you have to pay $10, $15 and it's minimum, absolute minimum. Some transaction takes $1,000, which is obviously too much.

[00:24:53] JM: There are defi applications that are actually using these alternative Ethereum-compatible networks today. There are smart contracts being deployed to Polkadot, or to cosmos and serving production traffic today?

[00:25:12] DE: Yeah. On Polkadot, I have to check if they have existing depths migrated to there. I know that, let's say, social swap, they – also on the Phantom, for example. They deployed on several chains at the same time, like Xdie, Phantom, Matic chain. Polkadot, probably they have their own ecosystem. Let me check.

Yeah, most of it, I see it's – some of them actually are – was on Ethereum, AdEx Network, for example, I remember they was on Ethereum before. I'm not sure if it was just a reboot, or somehow, they just mapped it to Polkadot. Most of it are just new, original tokens that are being developed directly on the Polkadot. So far, the most applications that they transitioned and migrated from Ethereum to Matic chain is – I mean, we're just dominating the space at the moment. Because even if we take Binance chain, Binance chain has mostly projects that were built on the Binance chain directly. In this regard, we're needing this space right now.

[00:26:52] JM: I've heard a lot about Binance and Binance smart chain. I don't know that much about it. Can you tell me a little bit about what it is that that piece of infrastructure does and what impact Binance has on the decentralized world?

[00:27:13] DE: Yeah. Binaance chain is – basically, it's a fork of Ethereum, client GIF. They modified it, so it works in proof of stake fashion, so you can stake B&B, their token to validators and I guess, earn some rewards. Here, I'm not sure. I think, Binance chain, since they saw that the bridge to Binance chain is not decentralized. It's pretty much the gateway to Binance chain is that Binance itself.

It's incredibly centralized solution that is basically a chain baked by Binance. The impact it does on Ethereum itself, I don't think it's inherently bad, because the Binance chain on its own, it didn't attract the existing projects. I mean, probably some of the projects moved, like harvest farm and some other projects. In general, it gave birth to quite a lot of absolutely new devs, just well deployed on the Binance side.

I think, in some ways good, because it's easy to onboard for the regular, or any new user, because you just get to Binance and Binance is the biggest exchange out there. Obviously, they have a lot of customers. Then, they just can go to Binance chain and do relatively cheap transactions. Because now, the Binance coin has increased in value, substantially increased, which of course, increases the gas price and US dollar equivalent.

Recently, the Binance chain, also experiencing this limited block space, because it's still Ethereum is just pumped a bit. There's bigger blocks basically and they are short in time, but generally, is the same Ethereum. It has the same problem. Once it hits the limit, the gas starts to skyrocket. Compared to Ethereum, it's still much, much cheaper transaction, even now.

Getting back to impact, I think it's good because any new user can just start using blockchain, some defi. He's not being scared away by Ethereum transaction prices and block time. In a way, it's good. It's not good in a way that it tries to compete with Ethereum. I think, it's not that big of a deal, because the layer two solutions on Ethereum coming and Binance chain will not be able to compete with whole Ethereum ecosystem eventually.

[00:30:52] JM: Okay, so revisiting Polygon. How does polygon compare to some of these other Ethereum-compatible alternatives, like Cosmos, Polkadot?

[00:31:10] DE: Okay. The main difference is that we don't build separate chain, that is basically compete with Ethereum. Instead, we derive the security properties of Ethereum. We are interconnected with it. Assets just can move back and forth. We just assist the new projects and projects that are running right now to scale and attract more users. I think that's the main difference. In a way, we look the same that we have this some child chains, like power chains, poly chains that are specific to the application, or for some group of applications, and that can be interconnected within the Polygon system.

The biggest difference that we are part of Ethereum itself. We combine and going to be combining the best scalability methods, like optimistic roll-ups, ZK roll-ups, proof of stake bridges, and always will be part of this gigantic ecosystem that will scale Ethereum way beyond it can achieve. We can scale it enough to meet the mass adoption requirements.

[00:33:01] JM: Is there a coin associated with Polygon?
[00:33:05] DE: Yeah. It's matic token. Because we were Matic Network before, so we have matic token. Then we have decided to rebrand Polygon to meet the our new direction better. Since the token is already written on chain, we can't really change it. It just stay as matic token right now.

[00:33:39] JM: Where is the engineering with Polygon today? What has been built and what's on the roadmap?

[00:33:48] DE: I don't know the details on the roadmap. We're still working on it. What is really is the better version of SDK for Polygon. That's some building blocks for spinning up the chains. We are working on the third version of the currently running matic chain. We plan to make it just better in a way that we want to go away from the original Ethereum consensus and make it better, suitable for proof of stake environment. Because now we run the Nakamoto consensus. That's basically Bitcoin consensus, original.

It's not really well suitable for high-throughput chains. We will use much better Istanbul BFT consensus, which is much more stable and faster in general. We also work on, like I personally work on data availability chain. It's a specialized chain that will bake our Polygon chains and can be used as blockchain as a service for other chains as well. The main purpose for it to solve

their data availability problem for layer two solutions. That's besides all their work around wallet and our infrastructure, working with inferior to scale our RPC nodes, because our usage of the network was surging during this week. It's just exploding.

One week ago, we were doing 700,000 or 600,000 transactions a day. Now it's almost 3 million. Yeah, when you build the infrastructure to handle the load. In general, yes, that's what we are working right now. That's big and tough tasks. They need some time and engineer work.

[00:36:22] JM: Okay. Well, we're nearing the end of our time. Maybe we can take a step back even further. I just like to get your perspective on where things are going and where we're at. In terms of defi today, defi feels very much like a casino. It's a casino that's running really, really well and really successfully and there's lots of abstractions there. How does defy get from a casino to a place that has a positive impact on the average consumer?

[00:37:00] DE: That's a tough question. Because I think, since it's just emerging technology, and all technologies like Internet, they're just get in through this bubble stage. Bubble stage is being led by its cameras, rack poles and all kinds of stuff. Back in 2017, there was ICOs, now is defi. I think, it's just a part of the evolution, I would say, like the cycle, when people got burned enough on a scale that finally, this depression stage will come and only, the real products will just arise from the ashes that what happen with Amazon, Google in the past.

Yeah. I think we're just not there yet. We're still in this gambling stage, bubble stage. Eventually, we will come there, because defi is a really great idea. It's a great tool, financial tool. I think, there is a future fundamentally. On a short-term right now, yes. As you said, it's like a gamble with play money all around. I think, that's just part of the journey. How long is it going to take? I'm not sure. I don't know. There is at some point, of course.

[00:38:35] JM: Cool. Well, that sounds like a good place to close off. Thanks for coming on the show and it's been a real pleasure talking to you.

[00:38:42] DE: Yeah. Thank you for inviting me.

[END]