**Hardware:**

\*D:  
We don’t need to introduce ourselves? Should we?

\*C:  
Y’all can. They already know who I am. They know me.

\*Music\*

C: Welcome to the Hashing It Out podcast, where we talk to the tech innovators behind blockchain infrastructure and decentralized networks. I’m one of three hosts, Corey Petty.

J: And I’m Jessie Santiago. This episode is all about blockchain hardware. How it got started and where we are now.

D: Dee Ferguson here. We’ll be talking to TrueBlocks founder, TJ Rush.

\*TJ: I love everything about the technology other than all the things I talk about.

D: And President of Vulcanize, Rick Dudley.

\*Rick: I’m gonna go on a slight tangent here.

C: This episode of Hashing It Out is sponsored by ZenGo. With Zengo, you can buy, trade, and earn up to 8% interest on crypto assets while enjoying 24/7 customer support. And no more private keys. With Zengo you’ll get two 'mathematical secret shares' – one stored on your mobile device, the other on the ZenGo server. With no single point of failure, if something happens to one of the shares, your crypto is still safe.

Download the ZenGo app and use the code Trade-Zen at sign up to get ten dollars back on your first purchase.

Music composed by Nate Ferguson.

Music Transition

C: We wanted to try and suss out this change from the original narrative of bitcoin, which was like one-cpu-one-vote, and like people running a bunch of stuff at home and how everyone participates in this network commensurate to their ability to have one-cpu or multiple-cpu’s to where we are today which is drastically different.

­

What is your take on that? How do you see the evolution of starting from this concept of one-cpu-one-vote and the hardware implications of that, to what it means to even run infrastructure today?

R: Yeah, I mean I think one-cpu-one-vote was a great idea, a great aspiration, a great hope, a great narrative, but I don’t think it was ever really thought through all the way… or really early on it was clear that that wasn’t going to work and there would be centralized parties that were basically like banks. I know there is somewhere in Bitcoin talk, Hal Finny talks about Bitcoin banks.

So, I think that even though you could run bitcoin nodes for a while as an individual either CPU mining or GPU mining and eventually FPGA mining was, I think achievable by the end user. Like for the butterfly lab stuff, I wasn't paying that close attention at the time so I don't know the exact dates, but after that I think the idea of individuals having reasonable mining operations kinda went out the window.

Yeah, why do I think that happened? Ultimately it was like, I don't wanna say it was bad design, I want to say it was like it was more of an aspirational thing because I think the design, it is sort of obvious from the design. I mean the second or third comment in the original cypher pump mailing list is ‘You're going to boil all the oceans with this thing’. So, people kind of knew right away that it didn’t make a lot of sense.

Music transition:

?: TJ Rush got his first computer in 1982 but 2016 is when he discovered Ethereum.

C: How did that change over the years? Right? Cause I remember when it even started, you ran mist and running a node on your laptop or machine or whatever, it was relatively straightforward and simple. Um, that's not the case today and it's certainly not the case. That's certainly differentiated from when we started in Bitcoin and running a full Bitcoin node in your laptop was easy. And you can mine, so like walk us through like your past in trying to run this infrastructure locally and build local first applications and how that's changed throughout, like just your, your experience in this ecosystem.

TJ:

So, the first, the first thing that you had to do was run mist you would download mist and run mist. And it was called a web three browser. And inside of mist, it started up the, the, um, geth node basically. And it had so it had its own API endpoint called local host, 8545, which served the RPC to mist. So that was in maybe March of 2016, maybe February, March of 2016. It took about, you know, a day or half a day to start a brand new installation of mist and then, you know, fast forward to about, um, late 2016 and it starting to take, and there was this really huge, um, D-Doss attack in October of 2016. And what happened is someone created about 20 million accounts over a 10, 20 day period. And then they had to clean up that , D-Doss, which was another 20 million deletions of accounts.

So, what happened is the synchronization of the node went from kind of like this. It was like growing and then it went straight up kind of. So it went from a day, a day and a half, two days, three days. And then everybody started complaining about keeping this node in sync with the network. And I remember Joe Lubin and Consensus in New York were writing all kinds of different pieces of software, 20, 30 different projects going on. And every one of them was struggling to get users because they'd have to tell them, get the mist browser synchronized for five days. And everybody's like, what the hell are you talking about? So, um, Joe Lubin solution was a reasonable one, which is he's going to stand up Infura for everyone so that people don't have to synchronize the node and they don't have to worry about that whole thing. And I remember thinking at the time, and I even said this on Twitter, probably you can find it somewhere. That's a really bad idea. That's a, that's a bad idea because what you're doing is you're literally destroying exactly the thing that a decentralized network is, which is, you know, local node software running locally, and it's turned out exactly as I kind of thought it was gonna turn out, which is no one runs a node because not because they don't want to. Not because they don't think it's interesting cause they don't have to like, why would they run a node? There's no reason whatsoever to run a node. So, um, now I actually don’t agree with that. I think there are huge numbers of reasons to run a node but the community doesn’t seem to think that’s true anymore.

BREAK 1

D:

Do you think that the hardware limitations are what make it so easy for a user or consumer to say, nah don’t have to do that.

TJ:

There’s a whole bunch of reasons. That’s certainly one of them, the requirement on the hardware is onerous, it’s really difficult. It’s also, you don’t have to, it’s like there’s no impetuous to do it. For me what that does is it changes the nature of the possibilities that you have because Infura is shared among a hundred thousand people, or I don’t even know how many people per minute or whatever.

So, no matter how much resources Infura has they are incentivized to deliver as little bandwidth as possible to each individual user because they want to keep their costs down. So, what happens is, you get applications software that can’t really operate the way a fully local piece of software would operate if you had a local node. So when I run true blocks, which is my project, I’m running against a local node, I hit the node 20 thousand times a second, or however many times I don’t know exactly, but a hundred times more frequently than anyone can hit Infura without getting rate limited. So, the nature of the application that you can build when you have a local node is just a completely different thing than the nature of the application you build when you’re hitting a share resource like Infura. That, to me, is what it means to be decentralized.

It’s decentralized, so the benefit of running a node locally to me is speed and not sharing and not being rate limited and not paying 350 dollars a month if I want access to every piece of data on the chain, which I have to do if I use Infura. I don’t have to do if I’m running my own local node. But all those things go away and people’s attitude towards the things we can build, they just atrophy. They just disappear. People don’t even imagine the possibility of building a different kind of application. That to me is the worst outcome of Infura. And I don’t mean to hit upon Infura, it’s just the nature of the world. It just happened.

C:

You use Infura as the canonical example of centralization, right? There’s this new friction that we’re introducing with a decentralized network which is running your own node, maybe going to buy a piece of hardware that is larger than your laptop. You’ve gotta, you know, prevision it, set it up correctly, make sure it’s online, make sure you have enough bandwidth. Those things have changed over the years in terms of the requirements to do so. So instead of that, in lieu of that, we’ll do it for you.

TJ:

That’s right.

C:

And there’s a tradeoff there and you mentioned one of those tradeoffs now which is you get rate limited so its within their benefit to minimize cost to serve you just as much as they have to in order for things to work and that limits creativity and building applications.

TJ:

Exactly right.

BREAK 2

J:

Where do your thoughts lie on a lot of these L1’s not providing hardware minimums that allow people to run the hardware themselves. How do you feel about that?

TJ:

So I was saying there was this big D-doss attack in 2016 and then all through 2017 it kind of settled down and cryptokitty comes in late 2017 and again you get this spike in how long it takes to synchronize the chain. Then I was running open Ethereum at the time and I had like a regular Macintosh or something and then it started getting up to 2 terabytes of data. I went out and I had to buy a new computer for ssd drives because it stopped working on regular hard drives. I went to the store and I just told the guy I want a really powerful gaming machine and he just built me this lennox box that was basically a powerful gaming machine because I didn’t know how else to describe what I needed. And it had like a 4 terabyte hard drive so that lasted until the middle of 2018 and then it just kept growing and kept growing, the size of the hard drive needed. Pretty soon I had a 14 terabyte hard drive on my lennox machine, right.

J:

Which you used for pulled storage?

TJ:

There was, I don’t know the technical details, I’m not terribly technical with the hardware but it was a raid zero thing and I had actually two lennox boxes in the same machine. This was open Ethereum and at the time, this was now about 2020, so open Ethereum was taking up 12 terabytes because I run… my software wants to look at the history of every address so I’m running an archive node and I’m enabling tracing so it’s really the worst case scenario for this size. It’s not true of a regular user who would just run the front of the chain. I’m a total different animal there.

17:28

But then you start to look at Eragon. And Eragon, the node software called Eragon, this is all Ethereum main net I’m not too knowledgeable about other chains. Eragon takes a 12 terabyte database and turns it into a 1.1 terabyte database and I can get exactly the same data from that node software as I could get with open Ethereum. I’m like, first of all that is totally not possible to do, but he did it. So, I don’t what magic he did inside of his code, but he probably set back the clock five years on this issue of how hard it is to run a node. So, all the other node software, if I understand it right now, for an archive node is still 12 or 13 or 14 terabytes. Which, if you think about it from Infura’s perspective that’s a disaster for them as well. They can’t be running separate nodes, they’re not putting 14 terabytes of data on every one of their endpoints. There’s no way. So, what they’ve actually created is some piece of software that stands in front of the node and you’re not getting access to the node, you’re getting Infura’s version of the node. Which to me is literally google. It’s literally google. So, Eragon comes out and kind of saves the day. They push 12 terabytes down to 1 and a half terabytes and it’s now grown into about 2 terabytes now so I have like 8 extra terabytes or 10 extra terabytes on my machine so I’m happily just running along for a couple of years without having to worry about it, I hope.

BREAK 3

TJ:

But let me say another thing. Now comes Ethereum 2. I’m like oh my god now I can’t even use Ethereum one clients without running Ethereum 2 as well. It just got twice as hard. Not only for me but also for Infura. It got twice as hard is they’re going to run these nodes. I think what happens is people… they have other priorities is the thing. They just don’t have the priority that says run local nodes. It’s just not a priority. To me it’s literally the only thing that we all need to do. I’m probably crazy but, I don’t know. Do you guys think it’s necessary for people to run nodes or is that kind of radical idea?

J:

I run my own nodes. I have a server… Corey does it too.

C:

Oh yeah I run a bunch of different nodes for different chains.

TJ:

You run an archive?

C:

Since Eragon I haven’t archived. Eragon made it very simple to provision consumer hardware to run nodes. That was one of the things that like was difficult for people. Not only, some people don’t have access to this consumer hardware to run a node and most circumstances, even if you take… the EVM scales kind of terribly in terms of in resource cost as it grows.

Bitcoin is really good in terms of scaling resource costs if you take out proof of work. But like, the success of the network increases the computational costs, in most cases, of running the network. So people who get excited in the early days run things on whatever hardware they have available to them. Like right now you can run, at least with nimbus, you can run Ethereum 2 on a raspberry pie. That is not advisable because eventually you’re not going to be able to do that.

TJ:

Right

C:

So, you have to go out and buy new computers and so on and so forth. So, I think we have this situation that I find interesting. I think it’s very important that people run their own nodes but I’m also realistic in the fact that some people don’t have access to these things. They’re not easy to provision today. So, like today getting your node, getting the computer’s cool, getting it synced, like installing the software, getting the chain synced, making sure it’s up, making sure it's up to date, getting notifications that you need to make an update, etc.

That’s all cognitive load and skills that some people don’t have. That makes it more difficult; or they don’t have access to the hardware to keep up or they buy it and then they can’t actively grow it. Right? Because there’s been circumstances where I have a hard drive and I used it and the chain fills it up and I have to figure out how to migrate it. That’s… do I have to start over? That’s annoying.

So, I think that’s interesting, right? These computers that we have to run these nodes, and it’s very important if we want these networks to be different in any way from the internet that they set out to kind of replace or transform or change we need people to take responsibility by running their own nodes so we can build new types of software like the original internet, but it’s hard. I don’t know… like… just by experiencing it from the beginning of bitcoin to today and you look at the available chains outside of bitcoin and Ethereum like Algorand, avalanche, cosmos, polka dot, like all these different chains they all have their own computational complexity and computational resources to run these things. And if you want to participate in a multichain world then you need to run all of them. So, like are we expecting people to have server rooms and all gigabyte bandwidth?

Music Transition:

?: Rick Dudley says there IS a solution to reduce the amount of hardware you need to run multiple chains.

R:

I had an argument when I worked at consensus in 2015 and we were talking about proof of stakes and all these things, I think that is what the conversation was about. I was like ‘Guys money is centralizing. If you don’t want a centralized system don’t allow people to buy the tokens. That is actually the solution. Don’t sell them, distribute them some other way, otherwise you’re always going to have the centralizing influence of money’. There are billionaires, right, a billionaire has billions of dollars, there are people who have no dollars, they are going to have billions of times more power in the system. So, money is centralizing, so as long as people can buy hardware then it’s going to be… money is going to be centralizing.

So, that’s one comment. I guess the other comment is, stake growth in Ethereum is a mistake. The design was supposed to have check pointing and truncation and we still argue about adding that into the network on a fairly regular basis. We can build blockchains today that use checkpoints that have a fixed size of their stake. I think it’s called ‘Mira’ now. It is an extreme version of this. Their blockchain stays the exact same size as some number of kilobits, which I think is way too small, but you could make it arbitrary size. You could make it 500 gigs, 3 terabytes, you could make it whatever you wanted. We have the technology to do that, we know how to do it, people just haven’t implemented it. We could implement that on Ethereum today basically, it’s not super hard, people just choose not to implement that which is very annoying for me, personally.

C:

Why is that annoying? You don’t like the concept of, of, like people don’t like that because of the original narrative of being able to build from genesis with confidence and the… what is the word I’m looking for? The counterparty risk of trusting people for data and I’d imagine those systems either get rid of the data so you can no longer do that, or they use some type of cryptography to give you a different way of trusting the system.

The reason it is super annoying to me is that it doesn’t fit into any data storage strategy that exists anywhere. Librarians can’t store data this way, banks don’t store data this way, enterprises don’t store data this way, no one stores an immediately available monotonically increasing data set. It doesn’t make any sense. It’s literally not operable. You can’t run a system that way. We don’t have infinite disks and saying ‘Oh we’re growing slower than the rate of disk size increase’, Moore’s law applied to disks or whatever is like a bizarre cop out. Just build a system that allows people to use offline data, near line data, far line data, blah blah blah, which is like a well-established enterprise practice. It’s one of those things where it’s like ‘Oh you people are fake’ because you’re not even addressing this basic issue of how do I operate this blockchain as an operator?

D: So, you mean to tell me for a while now we don’t need to have a super growing blockchain that grows forever and I have to constantly update my hard drive space, and that is a thing that exists and we’re just not doing?

R: Yeah. Why would a client need to work that way? Does the data set increase over time, the historic data set? Yes, it does. Does the state object that Ethereum has for example, does that grow over time? That’s harder to say because, in fact, it’s difficult to even meter or monitor that object. That’s one of the things we do at my company. It is actually quite difficult to know what the Ethereum state actually is.

But, you could say ‘Ok, every year on Jan 1st there is a block number, we pick that block number, we generate a check point from that block number, and then a week later we publish that hash and we publish the state at that hash and then we don’t require the nodes to have any more data from the past’. People can just take that, put it on a tape drive, store it on archival tape, store it on a tape, when they need to get it they can go to the closet, pull up the tape, put it in the tape drive and do their thing. We can just do that at whatever frequency we want it to. Every day, every year, or whatever, that is how real live production data sets actually work.

D: I guess that goes to what Corey said, at that point do you trust third parties, do you trust… well you don’t even need to really because if you’re keeping your own archives.

R: Think about it this way. We could just say, ok Ethereum is never going to be bigger than 500 gigs. Right, which you can fit on your pinky finger. Right, 500 gigs you can fit on an SD card. You can say ‘any time we go over 500 gigs we start this tape backup process and we take a snapshot and we build the tape backup and then we add the checkpoint into the new chain and you can truncate all that data. I’ve written, I mean we’ve developed this multiple times at Vulcanize, different times as different situations. You can just truncate the blockchain.

­­

BREAK 4

J: So, I’m running a node for Avalanche. In fact, I just spun it up a couple of days ago, and when you’re talking about the problems associated with running nodes in a home setting it kind of like makes a lot of sense. I’m aware of this. I just know that a lot of people are curious. They… like I’m curious to just play around with it.

I’m wondering, for blockchains to have real application for whatever somewhat idealistic, but more practical applications, for maybe not a global computer achieving global consensus… Where is the practical implementation and what is the hardware that seems reasonable to be able to prescribe people to go out and buy, and to learn to maintain, and just to participate?

>

> \*\*R:\*\* You kind of mixed in a couple of different questions there. I think you meant it as one question but at the end you sort of like split it into three. So like, if you want to play around at your house with Avalanche then just buy the hardware to do that, that is fine. Just realize that eventually, just naturally, you’re going to have a very difficult time maintaining that node as your disk fills up basically. If you’re not doing pool management, pool disk storage, we use ZFS pools at Vulcanize. With a ZFS pool you can do things to help but ultimately, um, yeah and you could potentially run that for a very long time, like 20 years or something would be fine.

>

> In terms of what you actually need to run a smaller chain, you need practically nothing. You could run it on the cheapest computer you can… well like a raspberry pie or something. You could easily have a whole blockchain that all the nodes are just raspberry pies and you have the same level of security that you have with Bitcoin or Ethereum. That’s possible.

>

> They way that that would be possible would be to manufacture a proprietary asic and then distribute that proprietary asic in a judicious way and it would still be affordable. Basically, when people finally crack your asic and start competing in the asic market you either sue them, which is not cool or whatever but it would work, or you release a new asic. That would work, depending on exactly what you’re doing, that could be sustainable. It may be that you have so many nodes and you’re not giving out rewards, you’re not giving out any crazy rewards that end up inflating in realtion to the dollar in this crazy way, so no one bothers cracking your asic.

>

> Theres countless asics out there that have never been reverse engineered. You could say ok we’re going to sell these asics. We’re going to sell a hundred thousand of them and you can order replacements from us for a certain amount of time. They cost five bucks and we only give one to one person and be mostly ok. You can distribute via lottery or something, I mean theres all sorts of ways you could address that.

>

> \*\*J:\*\* Have as like a happy meal toy.

>

> \*\*R:\*\* Seriously, have it in one of those claw things where you have to get the stuffed animal with the claw, you could put it in there. You could distribute it any number of ways and it would be fine.

BREAK 5

J: Is it worth creating, like, a system of people that are not economically incentivized to remove the interaction of permissionless and incentivization as a civil mechanism. Is there a way to build, and just nobody has this answer probably, but are there better primitives in terms of cybil defense mechanisms that where there is like a little bit of economic gain but not entirely? Something that makes the whole thing more fun, I guess?

R: Well, you did it again. We could make a system that was fun and didn’t really, the fun-ness sort of overwhelmed the economic benefit. It’s funny, we’ve been talking for a while. I personally don’t believe that global permissionless systems make a lot of sense. Again, there’s a very, very, narrow use case. I think it’s great for gun runners. I think it’s great for, I mean I’m a black person in America, there’s plenty of times where people should break the law. I think it’s the ethical thing to do, but if you’re not trying to break the law, regardless of the ethics of it, the permissionless global transmission properties of bitcoin are very weird.

If I’m in a financial relationship with someone, I know that counter party, I’m transacting with the counter party, I don’t need to be incentivized outside of that transaction. If I’m trying to ship products internationally, across the ocean or whatever, and I need to use this illegal payment rail to do that, I don’t need to be incentivized to run the hardware any more than then the incentivization that I have of running my existing business.

So, you don’t, you don’t really need, you know, the incentive structures we have now are these sort of pyramid schemes because the chains themselves have no other utility. If I just wanted to use the chain to facilitate international business, which I think is a totally legitimate use case, a killer use case for block chains, I would say ‘Hey, you know, shipping company A, shipping company B, shipping company C, all you guys do deals together you guys work together, you have the same customers, bring your customers together and you work in the pacific, you work in the Atlantic, you guys don’t really compete. Let’s build a network together, I’ll give you all the hardware, you know, all the money you have to pay and all the opportunity costs, all the legal costs, all the friction, we’re going to remove all that by building our own monetary system amongst the 27 of us, or whatever, and you guys give me a sliding scale percentage of that so that I’m not, you know, in dune land floating around on all my money, and everything will be fine’. Right?

And there are people who do build products like that. Those products exist and they’re not talked about. I was surprised. I talked to one of the founders of skew chain. I heard about skew chain many years prior. I was like ‘Wait, that project is still around?’ ‘Yeah, we do billions of dollars a year, or whatever’. I was shocked, right? Nobody cares about that stuff but that is a perfect, legitimate, small permission system that couldn’t exist without blockchain technology, is a financial application, has benefits to its users and doesn’t have any pyramid or Ponzi scheme notions involved in it at all.

I think, generally speaking, proof of stake systems have this problem. This is why I’m interested in proof-of-stake and I believe you should know your counter parties. I imagine a proof of stake system has, you know, under 50 participants in it. They’re all named, they all know each other, they’re all comparable in some sense. It can’t be like there’s one overlord guy and then there’s a bunch of peons, that won’t work. They have to have some sort of natural quid pro quo, but they are also trying to underwrite each other’s transactions.

Another example that I’ve worked with over the years was royalty organizations for music. So, people that buy and sell music rights and get paid publishing royalties, it’s like a really sharky business and then they have this weird horse-trading b.s that goes on and it’s really inefficient you’ll notice music pop in and out of Spotify. The reason sometimes you’ll be able to listen to a song on Spotify and then a week later you won’t is because Spotify had the wrong royalty information in their system and there’s no global way… it’s like a huge mess.

A blockchain would sort all that stuff out and it actually would solve a problem that they realized they had in the 90’s and they didn’t have a technical solution. Blockchain is a technical solution to that. So those are the type of… so I think that yeah you need something like bitcoin and then you need a bunch of proof of stake systems, literally millions of them, and then they aggregate up and eventually have an ultimate settlement layer. Practically, I don’t think that will be Bitcoin, I think it will be Ethereum, but I think Ethereum will be this global settlement layer for this broad base of millions and millions of proof of stake chains.

MUSIC TRANSITION:

?: You’ll hear more from Rick about the future of scale and economics in blockchain in part two of this episode. Plus, how DAppNode got its start and what the future looks like to co-founder Edu Antuña and Business and Ecosystem lead Pol Lanski.

Part two drops August 21st. In the meantime, you can find Rick Dudley on twitter at A-F-Dudley-zero. Check out TJ Rush at trueblocks-dot-eye-oh and DAppNode at dappnode-dot-eye-oh.

D: Curtains! Close em!