EPISODE 551

[INTRODUCTION]

[0:00:00.3] JM: The Federal Reserve System is fraudulent. Whatever its stated purpose, its effective purpose is to create a mechanism of deficit spending by politicians through the most insidious invisible taxation of monetary debasement, a.k.a. inflation. Those are the words of Erik Voorhees, the CEO of Crypto financial exchange; ShapeShift. Long before he started at ShapeShift, Erik was opposed to some of the core principles of the global financial system, in which he sees the U.S. dollar as a means of control. As an early adopter of Bitcoin, Erik saw a way to make financial transactions without using fiat currency. Erik's company, ShapeShift, allows users to convert digital currencies between each other. Because ShapeShift only makes exchanges of currencies and does not hold much currency at any time, ShapeShift is resilient to hacking.

In this episode Erik and I discussed his economic philosophy and how that informs his affinity for cryptocurrencies. Erik also describes the architecture of ShapeShift and give some advice for how to think about building businesses around cryptocurrencies. ShapeShift has had a few near-death experiences like any startup, and there's a useful story in this episode about how to survive and recover from a serious business setback.

[SPONSOR MESSAGE]

[0:01:28.1] JM: Software Engineering Daily is brought to you by Consensys. Do you think blockchain technology is only used for cryptocurrency? Think again. Consensys develops tools and infrastructure to enable a decentralized future built on Ethereum; the most advanced blockchain development platform.

Consensys has hundreds of Web3 developers that are building decentralized applications focusing on world changing ideas, like creating a system for self-sovereign identity, managing supply chains, developing a more efficient electricity provider, and much more. So, listeners, why continue to build the internet of today when you can build the internet of the future on the blockchain?

Consensys is actively hiring talented software developers to help build the decentralized web. Learn more about Consensys projects and open-source jobs at consensys.net/sedaily. That's C-O-N-S-E-N-S-Y-S.net/sedaily. Consensys.net/sedaily.

Thanks again, Consensys.

[INTERVIEW]

[0:02:44.5] JM: Erik Voorhees is the CEO of ShapeShift. Erik, welcome to Software Engineering Daily.

[0:02:48.5] EV: Thanks for having me on the show.

[0:02:50.4] JM: ShapeShift is a technology company and a financial institution, and I want to discuss ShapeShift itself, but beforehand I'd like to explore your personal views on economics, some of the things that led you to starting ShapeShift. The first question is what are the biggest systemic problems with the modern financial system?

[0:03:12.3] EV: Wow! We're just driving right in deep to that question now.

[0:03:14.6] JM: Yes.

[0:03:16.2] EV: Okay. Well, I think the biggest systemic issue is that money itself, namely the dollar or in the other fiat currency, which is sort of as like the base protocol of the economy. Money is currently centrally planned and controlled, and we live in a allegedly market-based or capitalistic economy and yet the most important good, which is money itself, is essentially planned and controlled. I think that is hugely problematic. I don't think any person or group of people in the world is smart enough, wise enough or ethical enough to be in charge of something so fundamental to everyone's life. So that's really what got me interested in in crypto, in cryptocurrency, was that to have a market-based money as an alternative to a centrally planned coercion-based money.

[0:04:09.1] JM: Describe the most ideal world economic system that you think we could someday get to perhaps by way of these technologies that we're going to be discussing.

[0:04:20.6] EV: Well, probably the right answer to that is to take the humble path of not knowing what the right solution for everyone is. This is why I'm generally a free-market person, is it's not because I port to know how the world's work, it's because I don't know how the world's work, and I think people should generally be left alone to figure that out for themselves.

So I think that was impossible when money itself was controlled. Now that there is a way for people to have a free-market form of money, I think they can actually become more free in their own lives and we could actually see much more experimentation and allow people to live a more sovereign lifestyle.

[0:04:58.0] JM: Do you think it's an inevitability that we're going to get there or do you think there's some probability still that all of these technology could get stamped out?

[0:05:05.6] EV: I think it's inevitable. So what's not inevitable is which of these different cryptocurrencies will be successful. So Bitcoin could, Litecoin could fail, and any of these others could fail, but the ability to move value instantly anywhere in the world for essentially zero cost without anyone being able to stop it, I think that is a power that is inevitable. In other words, as the world — As people discover it, they will demand it and they won't settle for less than that.

So in the same way that once email happened, or VoIP or the web itself, it's just too powerful for people that it could have been stopped. There's no way to stop the web after the genie is out of the bottle. There's no way to stop email after the genie is out of the bottle. It delivers too much value to too many people around the world for it to be prevented forever. Now that doesn't mean that various governments won't interfere with its adoption or harm it in certain ways, but I think over time it becomes universal.

[0:06:05.5] JM: Let's say that a new U.S. president has just been elected and they name you, Erik Voorhees, the chief of crypto economic policy. What would you do?

[0:06:17.2] EV: Maybe first change my title away from chief of policy to be more like perhaps just a humble representative with some thoughts, and those thoughts would generally be laissez-faire thoughts, meaning don't set policy for something as complicated as a marketplace. Allow the marketplace to find its own policies through emergent order, and that's a very scary thought I think to people who assume that systems must be controlled from the center. But as I've grown older I've come to see how much order there is in emergent systems both in the natural world and in human interactions as well. Language being a really great example, right? So no one is in charge of language, but it has structure. It has meaning. It has rules and people follow them even though no one is forced at gunpoint to do so. So I think the concept of emergent orders is very important, and if I had a position of power like that that would be my primary platform.

[0:07:15.1] JM: I'm basically in agreement with you, but you must admit that there is some consequence of that emergent order such as perhaps people who have no idea what different tokens do buying these tokens that may have no value. People get wrapped up into Ponzi schemes that are clearly Ponzi schemes, and so it does because probably need to be some kind of policing of that behavior, right? Or do you just consider the financial pain that these kinds of people who get wrapped up into these Ponzi schemes suffer? Do you just consider that an inevitable consequence and perhaps we shouldn't be policing against that?

[0:07:57.1] EV: No. So fraud is illegal. Theft is illegal. These things are not suddenly okay just because they're done with a different tool, and they don't require some vast regulatory apparatus. If you are lying to people, misrepresenting something, that's fraud. So that's the kind of thing. They should be policed. I wish that's what the government would do. I wish they would go around policing fraud instead of making up thousands of pages of obnoxious regulation that punish the people who aren't out there frauding people.

[0:08:29.3] JM: So you have an interesting line on your profile from the Bitcoin talk forums. I don’t know how outdated this is, or maybe it's totally up-to-date. But it says democracy is the original 51% attack. What you mean by that?

[0:08:44.7] EV: Yeah. So I wish I could take credit for that statement. That's something that I saw I think back when I used to be on the Bitcoin talk forums a lot. Someone said that and I picked it up and ran with it because it was such a great saying.

I'm not really a fan of democracy and largely it's because the more power that a group of people have over an individual, the more dangerous that is. So if you think of the world in which you have an ultimate democracy, meaning you vote on everything, and nothing is protected. In other words, anything that the majority says goes. I think that's a really horrifying and dangerous world, and I think it was just a really nice representation of the concept of a 51% attack in Bitcoin. I think the rights of minorities have to be protected, and the ultimate minority is the individual, who is just one person. Against an individual, a mob mentality of democracy is a really dangerous thing.

[0:09:40.1] JM: Do you have an alternative model for government in mind is there no books that people can refer to study this concept in more detail?

[0:09:50.0] EV: I don't know that there is a better model for governance. Maybe there is, maybe not. The question is one of scope. So when I say I dislike democracy, it doesn't mean I would replace it with a king who is in charge of everyone's lives. What it does mean, however, is that the scope of what a democracy can act on I think should be minimized to the greatest degree possible. A local democracy in your town that has authority over the trash pickup schedule, the danger of that is highly limited, and in small groups democracy can actually work pretty well. The smaller the group, the more effective and reasonable a democracy generally is. So reducing the scope that democracies can vote in effect I think is the key, not necessarily that democracies themselves should be replaced with anything else.

[0:10:37.9] JM: The U.S. dollar is an inflationary currency. Inflation means that your dollars lose value over time. What are the pros and cons of inflation as a feature of currency?

[0:10:53.8] EV: Yeah. Inflation has become this thing that most people simply attribute as the like effect of nature or force of nature, like the winds and the rain. People are used to going to the grocery store, and each year the price of the food that they're getting inches higher and

higher and we just kind of learn that when we're little and we accept it and we expect that 10 years from now bread will cost more than it does today.

None of that is a natural consequence of markets. What it is is the natural consequence of printing money. So the reason prices rise is because governments print their money consistently and continuously which debases the value of it. It's not really that the things are getting more expensive, it's that the money you're using to buy them is becoming worth less.

Now, you can find all sorts of economists that will give you every justification they need to tell you why that's important, why governments need to inflate the currency, and most of it is just economic self-history. It's ridiculous. The U.S., for example, when it was founded up until about 1912 when the Federal Reserve was created, did not have general price inflation. So a loaf of bread cost roughly the same at the birth of the country as it did in 1900, and most people would be quite shocked probably to hear that, but it's true. And meanwhile, even without inflation, and this was of course it wasn't inflated back then, because dollars were backed by gold, which can't inflate. Even though there was no inflation in the general money supply, you had the largest and strongest period of economic growth that any nation in the world had ever seen. You had a country rise from essentially a small agrarian economy to one of the industrial superpowers of the world in 150 years all without an inflationary currency. I think that is a really good example of the, at minimum, how unnecessary inflationary currency is, and I would make the argument that it's worse than unnecessary. It is actually very harmful and damaging.

[0:12:55.6] JM: There is the argument that deflationary currencies result in people holding their currency, because if your currency is just going to go up in value, which is a characteristic of deflationary currency, then why would you spend it today? Why are some economists critical of deflationary currencies and what's your position on deflationary currencies?

[0:13:22.5] EV: Great question. So I would say more — It's not just some economists are critical of it. The establishment economists is highly critical of it. So it is the norm and it is the accepted truth that deflationary currencies are bad.

I disagree with it, and one thing I've seen that has been really interesting in the crypto world is this example of a currency, Bitcoin or some of these others, that not only gain in value a little bit

over the years, but gain in value massively. So it's not like next year Bitcoin will buy you 5% more than it does today. On average it might buy you 10-X what it does today. So it's like a very severe example of this effect. What you would expect is that no one would ever spend their Bitcoin on anything because of that. If that theory of this deflationary spiral was true and because Bitcoin rises so dramatically, no one should ever spend it on anything.

What we see is that that's not at all the case, that people spend it often and actually tend to spend the most during the periods when it is rallying the most. I think people in some graduate study classes need to do some analysis on this, because I think in Bitcoin you will actually find the disapproval of the deflationary spiral thesis, and it's been really remarkable to watch and you can get data on this stuff. You can talk to the merchant processing companies like Bitpay, and unequivocally they have the highest sales and the strongest growth when Bitcoin is surging, even though people know that Bitcoin will likely be worth more days or weeks later.

The fundamental reason is that money is not worth anything on its own, and it's only worth what it can buy. At some point you need to eat. At some point you need a car. At some point you need a home. So even though your money might appreciate over the next year, you don't just hold on to money forever without buying anything or you'll starve to death in a gutter. That's, I think, really that the critical weakness that the deflationary spiral misses.

[0:15:20.0] JM: And the data points that I hear people refer to when they talk about the problems of deflationary currency, the most common one I hear is something that happened in Japan at some point where when they had a deflationary currency. You compare that — Whatever, I don't know what event that was or when that happened, but that such is different set of circumstances than we have today. Like today we have e-commerce, and if we're talking about Bitcoin, we have a currency that is very much more divisible than whatever the currency was in Japan at that time. There're just all these other variables. I mean, the internet. Like there are so many other — There are things that have changed, and when you take the circumstances of an economy together with the characteristics of the currency, then you're running a completely different experiment than whatever was run 20 or 30 years ago.

[0:16:13.9] EV: Yeah. That's fair. Also, I think people need to understand the difference between monetary inflation, which means the printing of money, inflating the money supply. That's the

original definition of what inflation meant. The more popular usage of it, which means price inflation, which is the increase in prices in an economy. Obviously these things are related, but they're not the same. If you print a bunch of money, that's monetary inflation and it's likely to cause price inflation, but it might not. There might be other countervailing forces that reduce prices even though the money supply is increasing.

So when people say Japan had a deflationary currency, I don't think that's correct. I think they've had general price deflation among many assets, but the Yen, the Fiat Yen, is very much an inflationary currency and more of it is created every year than the one prior. So the terminology is really important.

[SPONSOR MESSAGE]

[0:17:15.6] JM: I love podcast, but even with podcasts I can get enough audio delivered into my ears, and that's why I use Audible. Audible is a leading provider of premium digital spoken audio information and entertainment on the internet. Audible content includes lots of audiobooks and other audio products. I mostly use it for audiobooks.

You can go to audible.com/sedaily and start a free 30-day trial. Your first audiobook is free, and that's the trial plan that I started on four years ago. Since then I have read a ton of books. I read a lot of business books, like *The Hard Thing About Hard Things* and *The Everything Store*. Right now I'm reading a book by Ryan Holiday called *Conspiracy*, which is about the court case between Gawker and Hulk Hogan. Sometimes I read self-help books. You've got your classics like *7 Habits of Highly Effective People.* Read that a few times. I read some history. I read about President Eisenhower in *Ike's Bluff*, which is an interesting story about how to avoid nuclear catastrophe.

So I really recommend checking out Audible. Audible.com/sedaily, would contribute to Software Engineering Daily's sponsorship health with Audible. I'm really glad to have Audible as a sponsor, because I use it so regularly and I hope that you do to. So go to audible.com/sedaily and check it out. You can also text SEDAILY to the SMS number 500500 and that will give you the same Audible 30-day free trial.

[INTERVIEW CONTINUED]

[0:19:10.2] JM: You've been harshly critical of the U.S. Federal Reserve. To quote you — This is from 2009, so you can let me know if this view is outdated or if you've become less extreme, but you said "The Federal Reserve System is fraudulent. Whatever its stated purpose, its effective purpose is to create a mechanism of deficit spending by politicians through the insidious invisible taxation of a monetary debasement, a.k.a. inflation."

By the way, we will get the ShapeShift eventually. I just really want — I find your views pretty interesting, so I want to go a little bit deeper. Describe your views of the Fed.

[0:19:47.3] EV: Yeah. I have to say the 2009 Erik Voorhees sounds pretty smart, because I would say that exact thing today. Yes. So the Federal Reserve exists to create money out of thin air, and I don't know to what extent the people that work there believes that or if they believe that what they're doing is important. I don't consider them a bunch of like sinister bankers who are trying to screw people. They may all be great people that really believe in what they're doing, but the effect of that institution is that they create money out of thin air, and this is economically destructive and harmful.

The reason it exists or why the governments allow such a group to create money out of thin air is because it helps the government. So governments generally spend vastly more than they have and they have three ways of covering that deficit. They can tax. They can borrow, which essentially just means tax in the future, and they can print money. So they're unable, for whatever reason, to ever live within their means. They spend more than they take in in taxes and they continually borrow more and more.

The third way of funding that deficit is simply by printing the money, and this is why essentially all large governments in the world have central banks and why they all do the same activity of printing money. It allows politicians to spend more than they take in in taxes, and I think that it's a horrible fraud, it's a scam and it destroys the value of capital. It destroys the value of people's savings over their lifetime for the benefit of the then current government and the contractors and institutions that build up around it.

[0:21:19.7] JM: Okay. Shifting the conversation to cryptocurrencies. When people try to pinpoint where we are in the evolution of this technology, they often try to compare it to the evolution of the internet. They try to draw these timeline analogies between cryptocurrency in the internet. Do you think this is a good analogy or do you think it's misleading?

[0:21:44.6] EV: I think it's a good one, but it's not perfect. It's good in the sense that the internet had a long history of development before it became widely known or used. Sort of in the mid to late 90s it started getting popular and by the mid-2000s it was pretty ubiquitous, but it had 10 or 20 year history before that.

Back then one of the reasons it wasn't used widely was because the infrastructure wasn't there, mainly like high-bandwidth connectivity, and the systems were just difficult to use unless you were a highly technically proficient. In that way, Bitcoin has looked very similar. It's getting better each year but it has been difficult for normal people to use and it hasn't had a lot of the infrastructure that has been needed to allow it to be used widely. Also, like the Internet, I think at some point it will become ubiquitous and it will seem obvious in hindsight, but until that happens, it has a lot of obstacles before mass adoption.

[0:22:42.3] JM: One thing that seems to make it a subpar analogy from my point of view, and you can tell me if I'm wrong, but it seems like back in the evolution of the internet we had deficiencies in the hardware. We had deficiencies in the physical infrastructure of what we were interacting with our information systems on. But today we've got that infrastructure, that the physical infrastructure is really well-built. The problem with cryptocurrencies is one of software. It's one of protocols and is a proof of work, is a proof of stake, it's politics. It's things that are arguably easier to figure out, because they're not bound by physical limitations, or maybe you would say they're harder to figure out, because they are issues of people, then there are issues of ideas.

In any case, it seems like if somebody came out with a software invention tomorrow that fixed scalability, for example, it would be like a step change in the usage, because that's really the limitation, or do you disagree with that?

[0:23:48.7] EV: You're correct that it's not a hardware level limitation at all. So in that way it's not similar to the internet, but I think the major obstacles to Bitcoin adoption are not scaling challenges yet. Those are more hypothetical and people that are already into crypto debate those heavily. But the average person is not using Bitcoin not because of scaling issues. They're not using Bitcoin primarily because they are already used to and comfortable with dollars and credit cards, and they are at the same time scared and nervous about the volatility of Bitcoin.

So those two things combined I think create a lot of pressure preventing people from trying to stuff out more thoroughly. The volatility gets sold simply with time and as the market grows. Bitcoin today is already much more stable than it was when I got involved. The last few months have been an exception, but it's generally getting much more stable, because it's a larger asset class and that will continue. Then it just takes time for people to change their behaviors. When people buy things online with a credit card, it works reasonably well. So there's not a huge impetus to switch, at least if you're an American, but in other countries you're going to see faster adoption rights, because they don't they a credit card alternative that works well. So they're going to be more willing to try out this weird new thing called Bitcoin than someone who's comfortable buying on Amazon using their credit card.

[0:25:08.8] JM: Okay. Makes sense. You run ShapeShift, which is a cryptocurrency exchange, and also a set of tools for people who are transacting with the cryptocurrency ecosystem. We've talked about your economic views. How do your economic views inform the direction that you set for ShapeShift?

[0:25:30.2] EV: Yeah, good question. Yeah, basically, ShapeShift is an easy way for anyone to convert one type of digital asset into another. So if you have Bitcoin and you want Litecoin or you have Ethereum and you want Dash, ShapeShift is probably the easiest way for you to make that trade.

I would say the way that it aligns with my economic views is that it doesn't try to dictate or determine which of these technologies is going to be the winner. In other words, I created it because I saw a new asset class forming. I didn't know which of these would be super popular or successful, but I figured the market would determine that over time. So building a tool that the market could use to express those preferences became an important thing.

So ShapeShift sort of is asset agnostic. It doesn't promote any asset over another. It just adds those which the market is finding useful and are seeing high trade volumes. Then over time hopefully ShapeShifter is helping the market figure out which assets are useful.

[0:26:33.7] JM: How do cryptocurrency exchanges like ShapeShift, how do they compare to traditional currency exchanges?

[0:26:41.9] EV: Yeah. Well, ours is pretty unique. So that question would be answered differently if I was talking about a traditional order book exchange, like BitFenix or Coinbase or Kraken or any of those. ShapeShift is different in in a few ways. One, we don't handle any currency at all. We don't handle dollars or euros or yen. We're only digital assets. Two; we don't hold any user funds. So every exchange in the world pretty much except for ShapeShift has accounts for people sign up and then they deposit their funds into that exchange, and the exchange is holding it all centrally. Then, by so doing, the exchange allows people to trade back and forth.

ShapeShift does not hold customer funds, which in my opinion much better from a security perspective, because even if we get hacked, we can't lose customer money. Because we don't have the customer money, it makes us less of a target to get hacked in the first place.

But, also, I think it's important from the perspective of what crypto is trying to do, which is to decentralize trust. It has been a great irony of the crypto industry that this amazing technology that decentralizes trust has had these huge centralized exchanges emerge that are holding billions of dollars in customer funds, and we've seen many cases where hacks or technical glitches have lost hundreds of millions of dollars.

From that perspective, both, so I can sleep at night not having to hold all that money. Also, from a more principled perspective, ShapeShift was built to be a fairly different model. ShapeShift, its model would not work with normal fiat currencies. It can only work using blockchains.

[0:28:17.7] JM: Why is that?

[0:28:18.3] EV: Because fiat currencies always have to be centralized. If you have dollars, they're in a bank account, which immediately means that they're held by some other party. With crypto, you can hold it yourself, and that fundamental difference allows different kinds of models to be built. For example, we could not use this current model if we wanted to add dollars to ShapeShift, if we wanted to let people buy Bitcion with dollars or any of that. We are simply natively digital. We stick with only digital assets and we don't touch fiat currencies or any of that stuff, whatsoever.

[0:28:48.7] JM: Right. This is basically because — When you think of holding funds, and this is for people who are less familiar with how crypto currencies work. When you think of yourself as holding funds, you're actually just holding the keys to those funds and all of those funds are actually — The state of those funds are maintained on the blockchain. Basically, when you say you have a wallet, wallet is actually not a good term for what a wallet is. A wallet is just a way to hold the keys which are your permissions to access the funds that are expressed on that decentralize blockchain.

So if I'm swapping Bitcoin for ether, for example, on ShapeShift, which is one of the things you could do. You can swap different cryptocurrencies for each other. If I want to take out some Bitcoin from my ownership stake in Bitcoin, I put in my Bitcoin address, I put in my Ethereum address and I input the amount of Bitcoin that I want to swap for Ethereum, theory because that's what ShapeShift, it's an exchange. When that transaction gets initiated, what is happening on the backend? Can you take me through some of the steps?

[0:29:56.3] EV: Yeah. The other piece of this that makes us different from a normal exchange is that we're not matching a buyer and a seller. We are always the seller. So when you come to ShapeShift and you have your Bitcoin and you want your ether, you come to us, you tell us how much you want and then we show you an exchange rate. If that sounds good to you, you send us your Bitcoin. So that's sort of step one, is you send your Bitcoin to one of our Bitcoin addresses.

As soon as we've confirmed that that Bitcoin has arrived, we send your ether to you from our wallets. So we're sending you our own property, because you sent us yours. That's sort of step one, and that's all that matters really to the user.

From a business perspective, what we're doing after that is that now we have too much Bitcoin and too little ether, because we just did a trade with you. So we then are going out into the markets and trading to get our inventories back to where we want. You can think of this as very similar to like any retail store that has an inventory of assets and they sell them to their customers and then sometimes they go repurchase that inventory, resupply. As long as they can buy that inventory for less than they sell, that's their revenue.

[0:31:05.4] JM: Right. So what were some of the challenges to getting that initial currency swapping system developed and deployed?

[0:31:13.4] EV: The biggest sort of thematic challenge is that, because we're natively on the blockchains and every trade happens on two blockchains, the one coming into us, the asset being sent to us, and the mass that we're sending out. We have adopted all of the scaling and technical challenges of these blockchains themselves and many of these are in various stages of alpha or beta level software. So we are running this software at a scale that the developers of these systems often have never been able to test themselves. For examples, ShapeShift is about 2% or 3% of all Bitcoin transactions in the world, thousands of them every day. So we just run into problems that just haven't been seen before, and Bitcoin is one of the most tested and bug free blockchains, but it's not perfect and some of the others are in much worse states.

So every time we bump up in sort of the scale of transaction flow, new problems happen. So a certain wallet that worked or a certain piece of software that worked when we were doing 500 transactions a day might spit out all sorts of crazy problems when we're doing 2,000 transactions, and then we might fix that. Then again, at 5,000, like a whole host of new ones.

Then the way that these things interact with each other is problematic. So like Ripple, for example, has to be entirely on its own server away from every other blockchain, because the software is just this resource hog and destroys any other crypto node that sits on that same server.

[0:32:48.0] JM: Noisy neighbor.

[0:32:48.7] EV: Yeah. There is there're like a gazillion edge cases of this stuff and it's just a constant challenge to figure it out.

[0:32:54.7] JM: So to be clear, you have to run full nodes of all these different currencies that you offer exchanging on?

[0:33:03.4] EV: Yeah. Many of these are tokens on one particular blockchain, like there're a lot of assets that are Ethereum-based tokens, so all of them exist on Ethereum. Yeah, we run full nodes to support all the assets in and out. Then at scale, we often have to have multiple nodes, because even if we're sending one Bitcoin transaction every 10 seconds, it might mean that there are 400 requests of the node every 10 seconds both trying to get the state of the wallet, the addresses that are generated, checking balances and like all the various things that happen to make one transaction occur. Then at some point we had to have parallelization between different nodes and set that up so that two wallets aren't sending the same funds to the same person at the same time. Those kind of problems can be very dangerous. So that's the — Yeah, that's the work.

[0:33:54.1] JM: Wow! So maybe this is out of your scope of expertise. I don't think you're a software engineer by trade.

[0:34:01.5] EV: Correct. Yeah.

[0:34:02.4] JM: But I'll ask you anyway. I mean, because most of the shows that I do are like I'm talking to some infrastructure company, or I'm talking to some company, like traditional infrastructure company, like Facebook has a — Okay. They've got some complex problems. But ultimately it's like kind of client/server model. You've got some databases. Okay. I'm sure they have some complex stuff, but what do you think are some unique infrastructures, so other unique infrastructure problems of having to maintain full nodes for all these different blockchains and having to scale them up and down and deal with — I guess, like you said, you've got race conditions between the different nodes. Do you have any stories or other canonical problems that keep coming up?

[0:34:49.6] EV: Yeah. One that a lot of people don't think of is simply the balancing of the inventory. So we're holding all these nodes and inventory of each coin so that it's immediately available when a customer wants to do a trade, and we also so that we can do quick trades elsewhere in the market. We have inventory at many other exchanges.

So what that means in real-time when you're at scale is that all these inventories of coins are constantly getting out of balance and they have to be moved between each other, right? So Bitcoin might need to move from Kraken, which is an exchange we plug back into the hot wallet or then some might need to be sent to BitFinex. That multiplied times 50 different assets 24/7 and five wallets per asset becomes a really crazy balancing act. Then, of course, the obvious answer is, well, just automate it. But when you automate the movement of crypto, it's really dangerous. You have to be very careful that things are getting sent to the right places, because if you automate a robot and he's spitting out your money into an address that doesn't exist, you can burn a million dollars Ethereum in five minutes. So that's been a hard challenge as well.

[0:36:04.6] JM: Do you have some humans in the loop on bigger transactions?

[0:36:08.3] EV: We are pretty close to having no humans in the loop or only with a little bit of oversight into things. It's largely automated at this point. Now is really a necessity. I mean, before we had some of these things ready, we had people staying up most the night just to be balancing things while customers were operating, and the damn crypto markets never close. So there's not like a Sunday where everyone can go home and have some beers and watch the football game. It's like the store always has to be open and it's a global business. So it was really — And everything grew so much over the last year and a half that that was really stressful I think for our company just on a personal level trying to deal with those kind of things as the engineering got built out.

[SPONSOR MESSAGE]

[0:36:58.9] JM: GoCD is a continuous delivery tool created by ThoughtWorks. It's open source and free to use, and GoCD has all the features you need for continuous delivery. Model your deployment pipelines without installing any plug-ins. Use the value stream map to visualize your

end-to-end workflow, and if you use Kubernetes, GoCD is a natural fit to add continuous delivery to your project.

With GoCD running on Kubernetes, you define your build workflow and let GoCD provision and scale your infrastructure on-the-fly. GoCD agents use Kubernetes to scale as needed. Check out gocd.org/sedaily and learn about how you can get started. GoCD was built with the learnings of the ThoughtWorks engineering team who have talked about building the product in previous episodes of Software Engineering Daily, and it's great to see the continued progress on GoCD with the new Kubernetes integrations. You can check it out for yourself at gocd.org/sedaily.

Thank you so much to ThoughtWorks for being a longtime sponsor of Software Engineering Daily. We are proud to have ThoughtWorks and GoCD as sponsors of the show.

[INTERVIEW CONTINUED]

[0:38:20.7] JM: You talk to any startup and they have some hair on fire moment or epic catastrophe where they think the business is done. It's dead. Something's gone wrong and there's no way to recover. I talked to John, your COO, I think, or he runs operations, and he was telling me about this instance where there was kind of — I guess you had sort of a vulnerability through your support team. Like you had a malicious actor in the support team somewhere and that led to a big catastrophic problem and then some down time for the entire system, and there were some doubts as to whether the company would be able to recover from that.

Can you tell you some about that moment if I'm recounting it correctly both from the perspective of somebody working cryptocurrency and also just as an entrepreneur, because I think there's probably a lot of software entrepreneurs out there that probably are going through something like that.

[0:39:20.5] EV: Yeah. Yeah, we actually publicized very well. It was in April 2016. We had an employee. He wasn't in the support team. He was actually brought on to do our infrastructure and dev ops, which is ironic, but he essentially stole a bunch of crypto from us. Again, we don't hold customer money, so there wasn't a risk of customer loss, but it was a pretty significant

amount for us. Since he was inside, we had to really reengineer and rearchitect a whole bunch of infrastructure after we saw it happen.

So the site was off-line, I think, for about three weeks and that was really stressful. I don't think there was a period at which we thought we couldn't come back. But when you're in that moment, you're wondering every day like how many customers you're losing and how many more days is going to be, and all the while you don't know which of your systems are all compromised, right? It might be one thing. It might be all of them. You kind of have to assume it's all them when someone on the inside was in there.

There's just a really like — There is a deep vulnerability that you feel as a person when that happens. It's very invasive and it'd be like if someone had been in your home and you didn't know how they got in or what they did, it's a very unsettling feeling. So that was rough. We wrote all about it and publicized the whole thing. I wrote like a 15-page blog posts about it called The Looting of the Fox. So you can Google that and read all about it. It's quite an interesting story and some both funny and tragic moments in there. But, yeah, that was certainly our hardest period as a company.

[0:40:59.1] JM: I will say this does highlight the resilience of the model that you've talked about already, where you just don't hold funds and it lets you sleep at night. Then the other side effect of this is you basically just have a business that's like an API and you just make money over time from that API, and even if you have some internal employee that steals a bunch of your money and walks away with it and disappears into the night, you've still got your software that you built. That's the amazing thing about software, is software has this incredible compounding interest effect where if you build software, it's very hard to disable that software as long as you have it backed up, and even if you lose some money, the software still runs. It still keeps making money and compounding interest. I think of software as a very unique asset in that way.

[0:41:54.2] EV: Yeah. It's a great point, and we've tried to engineer everything such that there is no central point of failure. I have to say that whole experience I think was really a validation of our model, which was that we – Regulators always like to talk about how well they protect consumers, which is largely – Frankly. We actually did protect consumers by building something

unique and entirely new model, and when we got hacked, everyone was protected not because there were some law about it, but because we built it ourselves.

Not only that, but we don't take customer information either. So when that hack happened, if we had been taking customer information, all that would've been stolen as well and leaked out on to the dark web and hundreds of thousands of customers would be dealing with identity theft issues. That was all avoided due to our model as well. I think this really demonstrates that the crypto and blockchains provide some really unique new business models that can be built that actually improves the safety of people not through some law that's written down by a politician, but through actual engineering and design work.

[0:43:00.8] JM: Again, I think it is worth emphasizing that this insight, the business that you built basically, like not holding funds. I think of it almost as sort of like the insight that Stripe had, where they're just like, "Oh, if you build a payments API that works really well and has really good documentation, this can be the foundation of a whole suite of products that you could eventually build." That's similar to what you're doing at ShapeShift. So after you got this currency swapping system working, you have expanded into multiple directions. You've deepened the functionality of that core competency, that currency swapping. You've built out an API and you also started spinning up other projects within the company.

So since you've got this wealth of opportunity, these different directions that you could go in, thinking strategically, how do you allocate resources between those different projects and particularly between the proven cash cows and the new projects that may or may not work out?

[0:44:05.8] EV: Yeah, really good question. So beyond ShapeShift, we have a few other products. We have coincap.io, which is a market data site for crypto assets. We have Prism, which is — It's a portfolio management system for crypto assets built on Ethereum smart contracts, but it's still in closed beta. We acquired KeepKey which is a hardware wallet company back in July of last. Then we have two or three secret projects that we haven't announced yet that are also getting worked on.

So all throughout 2017, we were very much faced with this question of like how do we allocate our scarce engineering resources, and we start hiring as fast as we could, but you can't just you

instantly bring in a hundred quality engineers to accompany. Doing that would be very dangerous, even if you could. So we had to make that decision of how much time and resources do we dedicate to these other projects, versus the core competency, the ShapeShift, which is making all the revenue and which is clearly the proven model.

So the answer for most of last year was to put everything we had on ShapeShift to make sure that it scaled and kept up with the demand that increased by 30-X over the year. Now that the current crypto bubble has popped for a little while, at least we are able to catch back up with some of the other projects that we want to work on, and it's been quite a relief. So I don't know that there's a great answer. I mean, we have projects that are awesome that suffered because we just couldn't put people on them last year. But I think ultimately you have to keep the core competency of the business strong resilience and everything else can come second.

[0:45:45.0] JM: Talking about recruiting and compensation in this world. I talk to Anthony Diiorio from Jaxs a couple days ago and he said that he actually does not give out equity in the company and said he has an interesting compensation model where he has kind of like a — It's sort of like a 401(k), but not exactly where he just gives people currency, and then they have like a currency portfolio over time. Anyways, interesting compensation model, but I also found it striking that he was just against giving equity in the company, but he found that people are inspired nonetheless. There's that question about the compensation. I'm also curious if it ties in how you retain people when you just have these occasional spikes where a bunch of your employees are probably going to get rich and maybe they'll leave. Yeah, I don't know. Curious about the compensation strategy and the retention strategy..

[0:46:40.8] EV: Yeah. Well, we definitely have more than a few employees who don't need to be here for their salary. Fortunately, in the crypto world, a lot of the people that work in it have an innate passion for it. So this is both helpful and that it's easier for us to recruit than an average company, because we're doing something that people are passionate about. It also means that we don't have to pay super elaborate salaries to get people, because there's an intrinsic motivation there. Then when people do get superrich on crypto, hopefully they don't all just leave, because they still care about the project.

We absolutely do give out equity to most of the roles at ShapeShift. There're certain time requirements that have to be here and certain performance metrics and all that, but I think we take a fairly opposite view of Anthony. We generally want people to have a stake in the company itself. So I've always felt that that was pretty important.

[0:47:33.1] JM: There's been a lot of conversation around stable coins recently. There's many different projects where people are working on stable coins. Then there's also the whole controversy around Tether, whether or not Tether is an illusion or a religion or what exactly it is.

[0:47:54.0] EV: A witch hunt.

[0:47:54.7] JM: A witch hunt. Is that what you think it is?

[0:47:56.6] EV: Yup.

[0:47:57.7] JM: You have faith in Tether. You have faith that it's backed by dollars?

[0:48:00.8] EV: It's not faith. It's based on seeing zero evidence of malfeasance or wrongdoing and seeing mob mentality gone amok at Tether. So I think Tether has a very simple model. They have bank accounts, and when dollars are put into those bank accounts they create tether tokens which are just blockchain assets backed one to one by dollars in the bank account.

So the critics all say — They say, "Well, how do we know that there's dollars?" And that has turned into this huge witch hunt where lack of proof in dollars has led to people assuming the opposite, which is that there are no dollars. Largely, this stems from the fact that it's been difficult for them to get audited, and I think anyone that actually runs a crypto company and has tried to work with auditors would have significant sympathy for that situation. Auditors and crypto is an awkward combination, even finding an auditor to do anything is hard, and then getting unqualified audits, harder still. So it's possible that the Tether people are running like the biggest scam in crypto that is ever happened. I think that's highly unlikely, and I hope at some point they can get through an audit and then actually disprove these rumors, because it's been a really obnoxious distraction I think for the industry.

[0:49:15.2] JM: Yeah, completely agree. It's interesting that your null hypothesis is that they do have those dollars to back Tether itself I think for other people.

[0:49:28.4] EV: I don't assume that. I don't assume either, but lack of evidence is showing either shouldn't lead someone to assume a scam. Like I haven't seen an audit of Coinbase's reserves. Why don't I assume that they're scamming everyone? It's because the mob hasn't gotten in a big tiffy about that one yet, but they have just as few audits as BitFinex does.

[0:49:48.3] JM: Interesting. Have you talked to anybody on the Tether team? Do you have any — I mean, I totally understand that the null hypothesis thing. But nonetheless, we all have our subjective estimations of people. So maybe if you've talked to them, and just by virtue of talking to them maybe you have some subjective opinions that these guys seem legit.

[0:50:08.6] EV: Yeah. I mean, I think it helps that I know most of the people involved both on the Tether side and on the BitFinex side, which is a partial owner of Tether. I know them, and just on a personal level I trust them to some degree. That's obviously not something that I can just communicate out to everyone, because trust is something that's built on a personal level between people. You can't share the trust in other words.

At the Satoshi roundtable a few weeks ago there was a couple guys from Tether and BitFinex there and we had a huge discussion with 200 people in the room, many of the industry leaders about Tether to try to clear the air. Hearing them in person and fielding questions directly from people in a room where everyone was there and present, I felt quite confident that they are not running the largest scam in crypto history. But it's really hard to disprove a mob especially on the internet especially when it is 100 times easier to create a bunch of angry tweets and Reddit comments than it is to refute them.

When the only reputation that people will accept is a full audit, and a full audit even when everything goes well takes a year, and if things are going well can be much longer than that. It's a really tricky situation. On some level, it's good that the industry is so quick to call things a scam, because that self- policing is important. It's sort of like an autoimmune response, but it often turns into an autoimmune disease where people just are going on witch hunts perpetually in trying to find all the bad people even when they don't necessarily exist. So it's a tricky topic.

[0:51:45.3] JM: Do you think you could be like a self-fulfilling prophecy where — I don't know, the SEC looks for a reason to sink Tether and then that ends up destroying what they've built even though they did actually do their best to keep things intact and to keep the one-to-one Tether to USD? I mean, how do you think this is going end, or will it end?

[0:52:10.5] EV: Well, they either have the dollars or it's the biggest scam in crypto history. If it's the biggest scam in crypto history, all the people involved in it are known. They're not anonymous. People know where they live. They know who they are, and all those people are very wealthy early adopters in crypto that run successful businesses. The notion that they would like perpetuate the scam just to get a little richer in a way that would clearly unravel, if it is a scam, it's essentially like a Ponzi scam and those have to fall apart.

So you essentially have a bunch of people that have a bunch of money already and run awesome businesses intentionally starting a Ponzi scheme and then perpetuating it for what? It doesn't pass the Occam's razor tests in my mind. What does pass the Occam's razor tests is that it's really damn hard to get audited and the witch hunts on the internet are really hard to counter.

[0:53:00.9] JM: I hear you. Although one analogy that always comes to mind for me is — So I used to play poker and there's this company called Full Tilt poker that you may or may not have heard of, where they had all these money and they were very wealthy people who were running it, and yet they still did these kinds of things where they would just sort of give out customer funds to people that were involved in the company. Then also with Tether, wasn't there some kind of hacking? Like the BitFinex got hacked and you could've had funds got stolen there and then they would be in a situation where they don't have enough funds to actually cover the Tether. I guess I'm not familiar with that.

[0:53:38.7] EV: With that hack specifically, there was some Tether that was stolen, and Tether is actually — The company is actually able to handle that really easily, because they can essentially blacklist those Tether coins that were stolen and just never redeem those for dollars. So that's actually I think a pretty nonissue, but it certainly didn't help their PR situation.

[0:53:57.6] JM: Okay. All right. Well, I mean, It's really nice to hear the counterargument, because I agree with you that there is not much evidence to accuse them, and I think we should have some counter arguments.

[0:54:10.1] EV: Again, I'm not saying that I know that they're legit. I'm just saying I wish more people would take a neutral position of, "Well, it's not really clear either way, and so I'm just going to reserve judgment." I wish that was a more common instinct, but often people just love to like latch on to any theory even if it's supported by a little or zero evidence.

[0:54:29.5] JM: Absolutely. I know we're up against time. If you were to take the opposite position on centralized banking — So if you were to put yourself in the shoes of the smartest banking bureaucrat that you know who is in favor of centralized banking, what would be the counter arguments that you would make against the ethos of Erik Voorhees? What are the strongest counter arguments against your ethos?

[0:54:57.9] EV: I think the most compelling argument that bankers do and will continue to make is that someone needs to be in control. I think this is the same impetus that leads people to follow religion. It's the same people — It's the same impetus that leads people to follow governments and kings. People feel like there has to be a leader or someone in control of things. I don't know what portion of society is open to the suggestion that certain complicated systems don't need someone in control, and actually are better controlled without centralized control, or in other words operate better, more efficiently, more safely without a centralized control.

So I think all that the bankers need to do is continue to remind everyone of what they already believe, which is that someone needs to be in charge of the money so that people are safe. That's really all they need to say, and I think any uncritical or unthinking mind will follow that as the default position.

So it's really on Bitcoin and on the crypto industry to demonstrate through its existence over time that there is an alternative there. It's not an argument that could be one in a debate. It's an argument that will be one in time with the evidence of the alternative existing and people seeing what it does.

[0:56:16.9] JM: All right, final question. As people start moving to cryptocurrencies and adopting it, what is going to be the response to these events from governments, or are governments going to make their own cryptocurrencies or are they just going to crumble? Are they going to merge? What's going to happen with governments?

[0:56:35.0] EV: Yeah. This was our favorite topic to debate on the internet in the early days of Bitcoin. To what extent will the governments just come down and try to destroy this stuff? Fortunately, the have not yet come down and try to destroy this stuff, and I think it's largely because a mix of economic ignorance and hubris. What I mean when I say that is I don't think most governments actually believe that their fiat currencies are threatened by this. Not yet. I think they don't understand that money is a good that will compete in a marketplace if there are alternatives. Thus, if there is a better alternative, people at the margins will start switching over. I don't think they see it that way. They've just grown up in a world where governments have been in charge of money, and so they just think that like that's how it will work.

So we'll see like how long it takes for them to understand that existential point, which is that if crypto really succeeds, it means replacing government currencies, which is really the goal in my opinion. Along the way they might try a number of things. I think some governments will try to make their own cryptocurrencies which will be really silly. I mean, they already have their digital currency. The dollar is already a digital currency, S what point is there for the government to make a crypto dollar? The only point would be that it exists on the blockchain and/or can't be inflated and/or can't be controlled, because those are kind of like important attributes of a cryptocurrency. The government is never going to make a digital form of money that they can't print out of thin air. That will just never happen and it will never make a form of money or payment system that it can't control centrally. So what's the point? I think a crypto dollar would look pretty much the same as the current digital U.S. dollar which exists in a in a bank.

[0:58:10.4] JM: Erik Voorhees, thanks for coming on Software Engineering Daily. It's been really great talking to you.

[0:58:14.1] EV: Thanks a lot. Have a great day.

[END OF INTERVIEW]

[0:58:19.0] JM: Users have come to expect real-time. They crave alerts that their payment is received. They crave little cars zooming around on the map. They crave locking their doors at home when they're not at home. There's no need to reinvent the wheel when it comes to making your app real-time. PubNub makes it simple, enabling you to build immersive and interactive experiences on the web, on mobile phones, embedded in the hardware and any other device connected to the internet.

With powerful APIs and a robust global infrastructure, you can stream geo-location data, you can send chat messages, you can turn on sprinklers, or you can rock your baby's crib when they start crying. PubNnub literally powers IoT cribs.

70 SDKs for web, mobile, IoT, and more means that you can start streaming data in real-time without a ton of compatibility headaches, and no need to build your own SDKs from scratch. Lastly, PubNub includes a ton of other real-time features beyond real-time messaging, like presence for online or offline detection, and Access manager to thwart trolls and hackers.

Go to pubnub.com/sedaily to get started. They offer a generous sandbox tier that’s free forever until your app takes off, that is. Pubnub.com/sedaily. That's pubnub.com/sedaily. Thank you, PubNub for being a sponsor of Software Engineering Daily.

[END]