EPISODE 933

[INTRODUCTION]

[00:00:00] JM: Cryptocurrencies are a fundamental computer science invention. Cryptocurrencies crashed in 2018 from a financial perspective, but the technology remains as promising as ever. Bitcoin is a decentralized currency and a plausible in-state that is implied by Bitcoin's current trajectory is a permissionless, decentralized financial system. This idea of decentralized finance or DeFi begs numerous questions.

Who will build the companies that provide the infrastructure for decentralized finance? Who will be the lenders? Who will be the credit agencies? Who will be the escrow services? How big will the teams need to be? Will these systems be built on smart contracts or can it be done with centralized cloud providers?

Haseeb Qureshi is a managing partner with Dragonfly Capital and a frequent guest on Software Engineering Daily. In fact, he's the most frequent, because he's a good friend and I really enjoy talking to him. He returns to the show to discuss his thesis on what kinds of crypto companies makes sense and how he thinks about investments into crypto companies.

Haseeb has written a detailed blog post about how to start a crypto startup and I recommend checking that out if you are looking for startup ideas or definitely if you are considering building a crypto startup yourself. If you're building a software project, post it on FindCollabs. FindCollabs is the company I'm working on. It's a place to find collaborators for your software projects. We integrate with GitHub and make it easy for you to collaborate with others on your open source projects and find people to work with who have shared interests so that you can actually build software with other people rather than building your software by yourself.

FindCollabs is not only for open source software. It's also a great place to collaborate with other people on low code or no code projects, or find a side project if you're a product manager or somebody who doesn't like to write code. Check it out at findcollabs.com.

[SPONSOR MESSAGE]

[00:02:20] JM: This podcast is brought to you by PagerDuty. You've probably heard of PagerDuty. Teams trust PagerDuty to help them deliver high-quality digital experiences to their customers. With PagerDuty, teams spend less time reacting to incidents and more time building software. Over 12,000 businesses rely on PagerDuty to identify issues and opportunities in real-time and bring together the right people to fix problems faster and prevent those problems from happening again.

PagerDuty helps your company's digital operations are run more smoothly. PagerDuty helps you intelligently pinpoint issues like outages as well as capitalize on opportunities empowering teams to take the right real-time action. To see how companies like GE, Vodafone, Box and American Eagle rely on PagerDuty to continuously improve their digital operations, visit pagerduty.com.

I'm really happy to have Pager Duty as a sponsor. I first heard about them on a podcast probably more than five years ago. So it's quite satisfying to have them on Software Engineering Daily as a sponsor. I've been hearing about their product for many years, and I hope you check it out pagerduty.com.

[INTERVIEW]

[00:03:47] JM: Haseeb, welcome to the show.

[00:03:49] HQ: Hey! How is it going, Jeff?

[00:03:51] JM: Today we’re talking about crypto startups.

[00:03:54] HQ: Oh, good! Wonderful.

[00:03:55] JM: Crossing two of my favorite topics.

[00:03:58] HQ: I was worried we might talk about that.

[00:04:01] JM: So we went through this 2018 bubble of –

[00:04:05] HQ: 2017.

[00:04:06] JM: Well, 2017, early 2018.

[00:04:07] HQ: Yes, 2017, 2018 was the bubble.

[00:04:09] JM: The crypto bubble of things which resembled startups in some way.

[00:04:14] HQ: Yes.

[00:04:15] JM: Kind of were startups. More like poor excuses for startups. The common lesson from 2018 was that none of this crypto stuff works at all, except Bitcoin. Maybe we should all be Bitcoin maximalists. Do we need crypto companies at all?

[00:04:34] HQ: Yes, we definitely do. I think it's tempting to sort of paint all 2017, 2018 as one giant bust. But the reality is a lot of things that came of age in 2017, 2018 we now have as important piece of instructor. Obviously, Ethereum kind of came of age in the ICO bubble.

But of course there'll a lot of companies in crypto that are not tokens, and those companies are important infrastructure. So things like exchanges, trading, lending custody, those types of businesses, they again also came of age during the ICO bubble.

So there are traditional looking equity businesses that did get created during that time, but most of the companies and most of the capital formation that happened then was kind of this weird bubbly blip and most of those companies may know fundamental sense. So it's kind of like all bubbles where Carlota Perez writes about this in her famous book on – I can't remember what the name of it is, but it's financial capital and financial revolutions.

[00:05:32] JM: *Hard Thing About Hard Things*.

[00:05:33] HQ: That's right. *Hard Thing About Hard Things*. Essentially what she says is that in any technological revolution there is always first a speculation period, then a collapse, and then a deployment phase. The speculation and the collapse, like the crazy bubble mania that happened, is essential for installing that technology and putting an infrastructure that is otherwise very difficult to actually coordinate its installation.

So the famous story about the Internet of like, "Okay, Yes. During the .com bubble, there were all these completely relevant businesses that made no sense that were totally over capitalized that were burning money without a real business plan."

But at the end of the day, it did lead to one enormous amount of consumer education about what Internet companies were. It led to enormous build out of mobile networks that were necessary to get the United States and other countries connected through Internet instructor, and that infrastructure paid dividends down the road of letting us adapt the Internet faster than we otherwise would. I think you're seeing something similar in crypto, is that if there was never an ICO bubble, there probably would not have been the level of understanding and engagement that you saw from the entire world in what is crypto.

What is blockchain? What do we need to pay attention to? Why is it important? There certainly would not have been the Libra, which may now be that that first beachhead of crypto becoming really mainstream.

The Libra would not have happened were it not for the ICO bubble. So it's a little too early to call how much of this is just completely wasted energy and how much of it is real installation work, but I think it is important not to paint the entire thing as having been a just kind of tulip mania.

[00:07:12] JM: Now that you're investing in crypto startups as well as crypto protocols, describe some of the promising domains that you expect to emerge as viable businesses within the crypto startup world.

[00:07:31] HQ: It's a tough question. It's intrinsically tough because crypto is such a nascent technology that it just moves so fast that I'm loathed to give a really tight rubric of what I think are the businesses that will exist. Most of my job as an investor is not to predict the future. It's to

understand the present, and that is hard enough. It basically moves as rapidly as this. Most of what's hard about investing is changing your mind in real-time and listening to when the world is telling you, “Hey! Your ideas about how this was going to go, they’re wrong now and you need to update your model of the world.”

So with that caveat in mind, I think a few of – The big categories I think crypto that really are true value and make for interesting businesses. One of them obviously is what we call layer ones. Layer ones are fundamental cryptocurrency public blockchains. This would be like Bitcoin, Ethereum, Tezos, Algorand, everything you see, EOS, TRON, all that stuff, that goes in the bucket of layer ones. These are fundamental cryptocurrencies that enable some kind of ecosystem or computational systems or contract system on top of them.

The second category, which I think will probably grow in importance over the next couple of years is what we call layer twos. Layer twos are systems that are built on top of these layer ones but are not themselves money or the originators of the security of the network.

Examples of this would be Lightning Network, Plasma. There are a number of other models that are becoming increasingly interesting to people such as what are called zero knowledge roll ups. There are other variations as well that people are experimenting with. There's a lot of stuff going on here that has been in the works of the last couple of years as a way of scaling these block chains without actually changing the underlying layer one, which is really interesting. It’s sort of like you have IP and the IP protocol is not going to change, but you can sort of upgrade TCP to QUICK, which actually has better performance than TCP in a lot of places, and there are ways in which you can –

[00:09:27] JM: Wait. QUIC is the UDP thing, right?

[00:09:29] HQ: I don't remember whichever one it is. The point is the same, that you can take the same underlying infrastructure and improve the protocols on top of it. I mean, take HTTP2 as a good example, right? Just simple things like multiplexing requests allows you to suddenly get a huge increase in throughput given the same underlying networking stack. The same thing sort of applies to blockchains. So that’s another area of active research.

The tough things with layers ones and layers twos is that people have been aware that this is a problem for such a long time, that there are so many projects in flight trying to solve the problem that any new startup coming down the road like in 2019, you're just going to be at a really big disadvantage in distribution and getting to market in time. So that's on the kind of fundamental core tech side.

Then there is the application side, and the application side is kind of – There are kind of two different routes you can go. So one is the on-chain economy, and then the second one is sort of the off-chain, kind of higher-level financial stack, the financialization of crypto. So that's the obvious businesses that everyone is aware of, like Coinbase, like Circle, like Gemini, like Kraken. These are exchanges, lending businesses, custody, the kind of infrastructure that you need to have a financial market built on top of crypto, which is a lot of the biggest businesses that we see right now that are traditional businesses, they're almost all the financialization of crypto.

But then there is the on chain ecosystem. This is like what is the economy that's developing on top of Ethereum or on top of EOS where everything lives in the blockchain ecosystem? Here we're starting to see an emerging ecosystem of – The most interesting of which is probably what's called DeFi or decentralized finance, and decentralized finance is that the idea that you can basically have alternatives to decentralized financial businesses like Coinbase or lending businesses and whatnot. You can have them entirely on a decentralized system.

For example, you can have exchange that entirely lives on blockchain. There's no business. There's no central operator who needs to run that business. It's all coded up in smart contracts and it serves its customers through the blockchain itself, and you can do the same thing with lending. You can do the same thing with swaps, with all sorts of derivatives, all sorts of tokenized financial products that live into a blockchain. So that's a new developing ecosystem that we are really interested in and that's growing really rapidly in crypto.

So that I think is a reasonably good taxonomy of what's going on in this space, but of course there's a lot else that I'm not talking about like tokenization, gaming, lots of on chain to off-chain things that people are experimenting with. So it's a big space, but I think those are the biggest categories.

[00:12:03] JM: You seem pretty non-dogmatic in terms of which of these things will or won't work out. I've looked at the layer two, layer one stuff for a long time and it's funny because the layer one people will be so convinced that it's all going to be layer one. The layer two people will be so convinced it's going to be layer two, but it's so unclear, and they're obviously just aligned with where their incentives lie. I mean, to some extent I guess they're just making arguments for why it should be layer two, which happens to align with their incentives. But is there anything you're dogmatic about this space?

[00:12:40] HQ: I'm sure many would people say I'm dogmatic about a lot of things. I try very actively to stay open and to let my mind be changed when the facts change. I think it's funny. I'd say that crypto Twitter rewards dogmatism. But investing does not reward dogmatism. Investing rewards keep an open mind.

[00:12:58] JM: But does investing reward activity in crypto Twitter?

[00:13:02] HQ: That remains to be seen. It's a little bit too early to say. I also suspect that the crypto investing world is also changing. Now it's growing up quite a lot. Where before it was sort of an old boys club of like there's a small number of people who are actually active in crypto investing. If you want to raise money, it was from one of this small number of people. Now, there are so many funds in the world that are chasing crypto deals that there's a lot of dumb money in this space, which also means that now you've got world-class funds like Andreessen Horwitz and Paradigm, which is sort of an outgrowth of Sequoia.

You really topped your funds with really serious talent who are working in the space. Obviously, I think my fund is in that category, and that just makes it that it's much more about being less dogmatic and being more open to seeing the world as it is and understanding the world more clearly and not taking sides in any of these ideological debates.

Crypto is very much driven by ideology, right? It's very intrinsically religious, and it's hard and somewhat unrewarding to be an anthropologist at a time when everybody is taking sides and getting ready to do holy war. So that part of it is tough. There are times when I'm envious of

people who do enterprise SaaS investing, because there's not much – Emotions run high in the enterprise SaaS investing world, but they do very much in crypto.

[00:14:20] JM: I don't know, man. You get into time series databases. It's a lot of time series databases.

[00:14:23] HQ: Maybe. I don't know. Yeah, exactly. Maybe everything was like that from the inside.

[00:14:26] JM: There are a lot of service meshes.

[00:14:28] HQ: Fair enough. Fair enough. Maybe I just don't know. Grass is greener.

[00:14:31] JM: The DeFi stuff, the centralized finance, the idea of a decentralized Coinbase. You and I were talking yesterday about coordination problems and how crypto only solves a very specific kind of coordination problem. Many of the imaginative crypto startups, Bloomberg for crypto for example, maybe they will work, but supply chain for crypto. We could maybe squint and find an incentive alignment problem that you can solve with crypto or crypto in its currently conceivable form. But many of them are – Man! You really have to squint. You have to squint and speculate and roll dice and stuff. So why is decentralized finance at all appetizing to you?

[00:15:19] HQ: Let me start answering that question by mirroring your sentiment, is that I totally agree, and I think a lot of these companies, these are a fast follower startups that came about after the ICO bubble seems still persist as sort of that ideas that keep floating around the collective unconscious that people keep trying to build. It's sort of like blocking for X, where there was like Uber of X and there was Facebook for X. There's a lot of blockchain for X.

The problem with most of these blockchain for X startups is that essentially the idea is we should get everybody on a shared database. That's the startup idea. Let's get everyone on a shared database. I agree. That's awesome if we could get everybody on a shared database, but getting everybody on a shared database startups are hard not because of the technology.

They’re hard because of the coordination problem. So let's say, “Great! Now you have a blockchain.”

You still have the problem of getting everybody on that shared database, and that's hard. It's not hard because they didn't have blockchains yet. It's hard because it's hard to get people to coordinate who fundamentally don't want to or for whom it's fundamentally hard to get a bunch of people, round them all up and get them to use the same technology.

I think these startups so far, like almost none of them have succeeded. That naturally might make you ask questions like, “Okay. Why is DeFi any different? What’s so interesting about decentralized finances? Isn’t that’s basically the same thing? Just finance but plus blockchain?” I think the answer is there's a very, very resounding difference between those two ideas.

So blockchains were first invented by Satoshi Nakamoto to solve one particular problem, and that problem was how can you create decentralized money? So far, a lot of people, myself included, looked to that and thought, “Wow! That's amazing. I bet there are a lot of other coordination problems you could solve using a blocking.”

So far it doesn't really seem like that’s true. So far it seems like the primary new thing that we can do, thanks to blockchains, is create decentralized money and otherwise decentralize in programmable money platforms. That is genuinely new. The outgrowths of that, of basically allowing global permissionless innovation on top of money, that has never been possible before.

What does that mean? What does that entail downstream? It means, for example, that right now if you look at DeFi, a lot of what's interesting in DeFi is like basically [inaudible 00:17:40]. People who were early investors into Ethereum who own a bunch of it and play around with all these daps that are kind of shitty to use for everybody else. They want to go long on their Ether. They want to lend it out. They want to do something weird that most normal people don’t really care about. That’s a lot of what DeFi activity is today. You might think, “Who cares?”

The terminus of DeFi is ultimately the idea of totally democratizing financial markets. It's basically saying that using DeFi you can create any kind of synthetic asset that you want. You create a stable coin, which is synthetically back the U.S. dollar. You can create an asset that's

pegged the price of gold, pegged the price of the S&P 500, like UMA protocol is doing. You can create any financial asset you want. Ultimately, a financial asset is just a price feed. It's a price feed plus some kind of stability mechanism. We have those. We have both of those.

With that, you can essentially build a financial system that anybody in the world can use just by having an Internet connection. That's big. Imagine an old lady in India, okay? So my parents are from Pakistan, India, kind of very similar culture. Everybody there, they don't really trust rupees. Okay? Their government is fairly nascent. It wasn't that long until they broke the grassroots colonialism. Very volatile, lots of capital controls, and basically every family will hoard on to their inheritance and gold. Gold is the thing that they trust. It's just generation after generation. Everybody trusts gold more than they trust anything else.

Imagine those old ladies who are hoarding all these gold. If they had access to financial markets outside of India, do you not think that they would just buy U.S. bonds or hold U.S. dollars or a diversified asset, a diversified set of currencies and stocks and bonds? Why would they not want the same portfolio that you want? Of course they do. They just don't have access to it.

The idea of DeFi is that it uses crypto. It uses the decentralized censorship resistant networks to create access to financial markets anywhere in the world, and with it, anybody can build on them. Anybody can do whatever they want. Ultimately, the beneficiaries of that are people who don't currently have access to them.

The instinct that a lot of people in the first world have is look at this stuff and say, "Okay. Well, why do I care about this? I'm not going to pay somebody using Dai or using Ether or whatever," which is completely correct. That is 100% right. People in the first world have such good access to financial markets and to financial services that nothing crypto can offer them is anywhere near as good as what they already have. But that is very untrue the farther you get away from the first world. Obviously, the vast majority of people do not live in the United States or in Western Europe.

So that to my mind is the best kind of intuitive sort of squint that you can take at the DeFi market and understand why, "Look. Today it's small. Today it's a burgeoning weird little place with a lot of crazy crypto anarchists, but it's going to be big."

[00:20:34] JM: I'll tell you what's cool about this, is when I look at DeFi and I compare it to the self- driving car. Man! I see less execution risk in DeFi. Maybe it will take longer for various reasons.

[00:20:52] HQ: There's a lot of regulatory risk, but execution risk is lower. I'd agree.

[00:20:56] JM: But it looks impossible and the limit to regulate. To me, I don't know, I don't know about you.

[00:21:02] HQ: I agree. I think regulation right now, today, all these things are kind of – They're kind of toys, and if the U.S. government really wanted to shut everything down tomorrow, they could get pretty close. They know the principals involved. They can find them. There's not that many people waiting to go to jail for DeFi yet.

[00:21:19] JM: It might accelerate the process.

[00:21:21] HQ: You're right. It absolutely might. But I think it's a matter of time when this stuff gets big enough and the stakes get high enough and the demand for it grows enough that I completely agree with you. It's not going away.

[00:21:34] JM: I mean, it's going to be so interesting to watch, because one of the really nice aspects of the crypto revolution, if you want to call it that, has been that it's like forced a lot of people to really examine what money is, which was one of those like weird – It's like you grow up and you're like, "Oh! Religion. No. I'm not into religion. I believe real things." Then you have these other things in life that sort of turn reality on its head. One of those is like a close examination of what money is.

[00:22:06] HQ: Yeah. Absolutely. I think crypto is very alien to anybody who's basically older than 40. Anybody who's under 20, I think crypto makes complete sense. Crypto is just much more intuitive to people who are younger.

[00:22:19] JM: It is the 2008 factor?

[00:22:20] HQ: It's a lot of things. I mean one obvious thing as being digital and native. The idea that money is not something printed by the government and that it's just like a number on your cell phone. T That makes complete sense. These people have never met a banker in their lives. Their relationship with money is very, very different from I think those of people who've lived through the 60s, 70s, 80s, getting off of Bretton Woods, all that stuff. It's a very different perspective on what makes money money.

[00:22:48] JM: You know what I was thinking about the other day? You experienced a currency debasement firsthand with the Full Tilt poker stuff, right? Full Tilt poker had a bunch of money and it was sitting in their coffers and they figured, "We're never going to run out of money. We can just borrow a little bit of this sum of money that's sitting in our coffers." Then it turned out that that would lead to insolvency and players were not getting paid out, and you were one of those players.

[00:23:22] HQ: Well, we did eventually get paid out, but many years later without interest.

[00:23:26] JM: Many years later when that territory got acquired.

[00:23:29] HQ: Yes. Correct.

[00:23:30] JM: I mean, I got annexed by the next largest financial monstrosity, which for all we know is doing the same thing, but probably not. Probably not.

[00:23:39] HQ: I presume that. Yeah, they probably have a tight leisure on them. I agree. I mean, it's funny though, like you said earlier that I'm not very dogmatic, and that's correct. I didn't walk away from Black Friday in the poker bust with like deep-seated animosity against the government. I basically was like, "Oh! Whoops! That happened. That's weird. Too bad I had so much money on poker sites."

The funny thing is like – My partner at Metastable, the fund I was at previously, he is Russian. He lived through the collapse of the USSR, and he has a very different perspective on money as a result of that. A lot of people who come to crypto, they come to crypto because they have a

scar somewhere on them that they don't show very often, but that really gives them a deep-seated skepticism and untrusting this when it comes to money, and especially government-backed money. I don't think I have that.

I think I come to this with a much more analytical. I don't have an axe to grind coming into crypto. I think the crypto is to change the way the money works in the future. I think it's going to change the relationship between central banks and their ability to control the money supply. I think there're a lot of things that are going to change in the world as a result of crypto. It sounds like I'm not really even rooting for either side. I think there are good points to be made on both. I want to see what happens. I think this is going to be an amazing show and I just have a bunch of popcorn in front of me and I want the best seat in the theater and options. I also want options. That's right. Low strike price.

[SPONSOR MESSAGE]

[00:25:10] JM: Looking for a job is painful, and if you are in software and you have the skillset needed to get a job in technology, it can sometimes seem very strange that it takes so long to find a job that's a good fit for you.

Vettery is an online hiring marketplace to connect highly-qualified workers with top companies. Vettery keeps the quality of workers and companies on the platform high, because Vettery vets both workers and companies access is exclusive and you can apply to find a job through Vetter by going to vetter.com/sedaily. That's V-E-T-T-E-R-Y.com/sedaily.

Once you're accepted to Vettery, you have access to a modern hiring process. You can set preferences for location, experience level, salary requirements and other parameters so that you only get job opportunities that appeal to you.

No more of those recruiters sending you blind messages that say they are looking for a Java rockstar with 35 years of experience who's willing to relocate to Antarctica. We all know that there is a better way to find a job. So check out vettery.com/sedaily and get a $300 sign-up bonus if you accept a job through Vettery.

Vettery is changing the way people get hired and the way that people hire. So check outvettery.com/sedaily and get a $300 at bonus if you accept a job through Vettery. That's V-E-T-T-E-R-Y.com/sedaily.

Thank you to Vettery for being a sponsor of Software Engineering Daily.

[INTERVIEW CONTINUED]

[00:27:00] JM: You wrote the pretty long post about how to start a crypto startup, and one of the things that struck me about the post was how similar it was to starting a regular startup. Is there anything counterintuitive about starting a crypto startup or is it just can I read the YC manual and follow that crypto startup will work?

[00:27:24] HQ: It's fairly similar. I mean, one departure from it is there are a number of elements you need to think about when starting a crypto startup that are pretty unique, such as where do I allocate my tokens? What jurisdiction should I build in? There's a lot of stuff in crypto that is more science project, which like building a protocol, or building a layer two system, or token economics, or crypto economics. That sort of stuff is pretty unique to crypto. It's not really a thing and most startup. Most startups, their economic models are pretty straightforward.

For the most part, there are more analogies and disanalogies. Part of the reason why I wrote the post is that crypto also is much more global. YC startup advice, while it's sort of old hat within San Francisco or in the Bay Area. Much less so outside of the U.S., and you notice that immediately when you meet startup teams outside of basically California and New York, that they have not really internalized many of the lessons, and kind of rightly so, because their VC communities are very different.

If you go to a place like Berlin, or Israel, or places even far-flung than that, the VCs do not have the same mindsets as the folks in Silicon Valley. So the start advice out here is just not appropriate for – I mean, it’s still good, but it's not sort of exactly what the VCs they are expecting to invest in. So it's tricky. It's a tricky game to play.

[00:28:45] JM: That's why Harry Stebbings stays in England.

[00:28:49] HQ: I can't speak for him. I don't know.

[00:28:51] JM: What about from the investor's point of view? How does investing in crypto startups differ from being a normal investor?

[00:29:00] HQ: It differs quite a lot. I think one thing that most people who've dabbled in crypto investing, especially who dabbled in it in 2017 will tell you is that it's very easy to lose your shirt in crypto if you don't know you're doing and if you don't have strong convictions and understandings about what actually drives value in the crypto economy.

There are so many smart entrepreneurs and great teams that are entering crypto now. Unfortunately, there're a lot of bad ideas, and it's very difficult to value a crypto company because most of them are valued on comparables. It's like, "Well, that startup before you was valued at this. So therefore you should be valued around the same." They're sort of priced rather than valued, because nobody knows what the valuations of these things could be, because for the most part, many of these crypto startups don't really have revenue. They don't really have clear monetization strategies. It's really, a lot of these are in the realm of basic science. The difficulty there is that if you don't have a keen eye for what is good science and what is bad science, you're definitely going to be lead very far astray. Also, there're just a lot of intellectual tar pits that you fall into within crypto.

So one of things I mentioned was like is blocking for X type things. It's very hard to understand why a blocking for X doesn't work. It's kind of like – I don't remember the name for this, but it's sort of like when someone gives you an argument and you kind of know – A conspiracy theorist. Comes and gives you some argument for why Hilary Clinton was something, something, something and you're like, "I know that's not true, but I don't care. I don't have the time like delve into why that's wrong and like where your sources are screwed up." You're smart enough to have developed an interesting tapestry that looks fairly robust of why this weird conspiracy theory must be true. I don't have time to debunk it.

That is very often true for a lot of these crypto startups. They're easy to believe. It's very plausible. It's hard to really know. Is this bullshit or not? I have no idea. A lot of time, my default

when I see that is to not invest, because if I don't actually understand how a startup makes money, then I truly positively believe what they're telling about the world, then I can't invest. I don't want to invest in things I don't understand. Unfortunately, a lot of investors do the exact opposite, is that if they – If it's credible enough that they can't discredit it, then they're like, "Sure. Why not? That sounds plausible. What if I miss the next big thing?"

That's really what drove a lot of 2017 obviously was like most of the great investors in crypto made very few investments in 2017. Most of the stuff that was driven up really crazy, none of the really great crypto funds were investing in any of that stuff. It was all kind of sort of dumber money farther down the stack that didn't really understand crypto that deeply that ended up really getting shafted when everything crashed. I think a lot of it is really just being, I guess, self-aware about the limits of your knowledge.

[00:31:49] JM: In our last conversation – Well, no. The conversation before that. We talked a little bit about the fact that in crypto you actually do not want to do the pattern of investing in a team that is really smart that's in a great market just even despite the fact that they have a bad idea, because that describes too many crypto people.

[00:32:12] HQ: Totally. I mean, ideas matter. It's this popular Silicon Valley attitude. They're like, "Well, execution matters. Ideas are whatever." That idea – I think I write this in the blog post. That advice is great not because it's true, but because it's useful. In reality, we all know that ideas matter. Of course, ideas matter. If you have a bad idea, no matter how long you grind on them, the only thing that you will walk away from is with the years of your life having been lost to that bad idea.

It still remains true that in early enough stage, great team with great ideas, even if their idea is not sound is worth investing and it's because that team will find the great idea and the great product through reiteration. But that is in license to just invest in ideas that make no sense given high-quality teams and high-quality products.

[00:32:59] JM: Okay. Great team, marginally credible idea, possible investment.

[00:33:05] HQ: It depends on the stage. It depends on the stage. It depends on the valuation and depends on how pliant that team seems to be to potentially changing their minds about that idea.

[00:33:15] JM: Blockchain for podcasts.

[00:33:17] HQ: Blockchain for podcasts. You know what for you? Anything.

[00:33:21] JM: RSS is kind of a decentralized – The way that it works is kind of – I mean, except it's all centralized –

[00:33:26] HQ: It's just a format.

[00:33:29] JM: That's true. Okay. The way it propagates is kind of – I mean – Okay. All right.

[00:33:36] HQ: All right. Just leave. Okay. Moving on. Moving on.

[00:33:38] JM: But it has a coin.

[00:33:40] HQ: It does have a coin. It does. We're starting that today. There is going to be a coin, RSS Coin. Get it here.

[00:33:44] JM: All right. Let's say I want to be working on a successful crypto startup as soon as possible. I'm in the crypto world, I'm bought in. Sign me up. I'm ready. I'm on the crypto rocket ship. I don't have a good idea. Should I burrow into a cave and do research for like six months? Should I go work at Coinbase? What should I do as a crypto person with no good ideas?

[00:34:14] HQ: I would say number one thing to do is to join the biggest, baddest, coolest startup you find that really gets you excited. That is by far the best thing that you can do if you really want to delve into crypto and get your chops as a crypto thinker.

Once you're at the point where you really understand the industry, then I think burrowing down and coming up with a bunch of ideas is totally fine. But a lot of the best ideas in crypto came

from people working on other stuff. So crypto is full of ideation all the time. It's pretty hard to be in this space and not be around people coming up with new ideas and new theories and new approaches to doing things.

So keeping it near the ground, but also improving your understanding of how things currently work, because crypto was really invented 10 years ago. It's like Cryptocurrencies. Almost all of the innovation in cryptocurrencies happen outside of academia. So there's no course you can take that's really going to get up to speed. There's no textbook. It's really just osmosis from all the stuff that currently exists and understanding how it works and why it was built the way that it's built.

So you can't skip that part if you really want to be adding on to the pantheon of crypto as it currently exists. The best way to do that is work on something. Work on something that already exists. Then the next stage once you're coming up with ideas, you're working with cofounders, building projects, going to hackathons, that's absolutely the right way to approach if you want to just crank on startup ideas.

But I think if you can be at a company while doing that, all the better. Because, again, the smartest people in crypto are the people working on this stuff and those are the people you want to surround yourself with.

[00:35:49] JM: You've been in Silicon Valley for a while and you've commented on certain cognitive dissonance and things and that's one thing I always find entertaining about your post and commentary and so on. One piece of cognitive dissonance that can really plague people sometimes is that they start companies for the wrong reasons. Why do people actually start startups?

[00:36:16] HQ: There are certainly a lot of reasons. I think over the last 10 years, startups have become really cool, which is terrible. It's terrible, because there are a lot of people who now see starting a startup as like kind of a rite of passage or sort of like another notch on their belt. It's kind of like being a Fulbright scholar or whatever. It's like being a startup founder even if the startup fails. Unfortunately, we as investors kind of feed into that, because we do give brownie

points to people who have started a start up at some point. So I can't claim to not be a part of the system in that respect.

But I think this notion that like everybody should just start a company at some point is kind of a bad notion for fairly obvious reasons, is that most people – That's a really crappy reason to start a company is because like you think you should. While it's good and we certainly should have more entrepreneurship in this world, I think being an entrepreneur for the sake of getting a badge of honor or looking cool or like beefing up your LinkedIn or being able to break in a product management or whatever it is that is convincing people to start startups these days I think is definitely a net – It's suboptimal I will say.

A lot of people start startups to make money. A lot of people do it because they want to be cool. A lot of people do it because they think that it's going to make them happy. Most of them find out that all of those things will not happen as a result of starting a startup for the vast majority of people.

The best startups are inevitably founded by people who actually want to change something in the world. People who see like, "Man! This market sucks. It's inefficient. It doesn't work. There should be a better product, and the product should look like this, this and this. Nobody is building it. So I'm going to go fucking build it." That's what the best startups tend to look like. It tend to look like products of just like overwhelming frustration of just like, "God dammit! Everybody else is an idiot. I'm going to go do this and fix this whole thing once and for all." That's what great startup tends to look like.

You pointed every great company in most sectors. They were not built by people who are trying to look cool. They were not also built by people who are just wanting to make money. People who want to make money– I mean, it used to be the case, people who wanted to make money will just go to Wall Street. Unfortunately, now they get diverted to Silicon Valley as well. So we've got our share of them.

But my take is that for the most part, I'm happy to see people working on startups, and it's pretty easy to tell when somebody is there for the wrong reasons. In essence, I'm not too worried about it, but are going to be people.

[00:38:37] JM: All right. Tougher question for you.

[00:38:39] HQ: Go for it.

[00:38:40] JM: Before you were working on Dragonfly, which very happy about you being there, and I think you're going to do fantastic. You were working on a stablecoin for a while. You are thinking about stablecoin. Well, I don't know if you –

[00:38:53] HQ: Yes. I was working on a stablecoin.

[00:38:55] JM: Working on one. You were working on that idea. Were there any cognitive dissonances there? Why were you working on that?

[00:39:01] HQ: I was working on a stablecoin because, one – So at the time, the only stablecoin projects that existed were terrible. There was BitShares, which had their USD stablecoin. There was one called Basis, which I wouldn't call terrible, but I would say that I didn't think that their model was sound in the long run. There was a team called Maker DAO, which at the time that we started working on this had not actually launched anything yet, even though they had raised an ICO many years earlier and they kind of were working on that thing for like 3+ years and they had not shipped anything.

So we just thought like why isn't there just a freaking stablecoin that's actually decentralized? So me and my cofounder came up with a design for a stablecoin that we thought would be good, and this is kind of where it came from. It was just really like we were looking at the different things that we could build. Honestly, part of it, to be quite honest, was that like I realized I don't like working at big companies, and startups are – I think I'm somebody who's abnormally well-suited to startups just because like I work much better in chaos than I do in highly-ordered situations.

I thought, "Hey, crypto is a space where like there's so many things to build and not that much exists yet, and I think it really should." DeFi in particular was something that I always found

really exciting. At the same time, I was really frustrated that nobody was shipping. Nobody was actually just building stuff.

Now I'm happy to say that that has really been ameliorative over last couple of years. Since 2017, basically around December 2017, Maker DAO launched Sai which then got rebranded to Dai, which is now the currently largest decentralized stablecoin. Stablecoins in general have really, really grown in the last couple of years. The ecosystem has gotten a lot better, but that moment in time was definitely a moment where I was like very annoyed at the state of how crappy everything crypto was.

I remember talking to you about this. My first instinct when I saw crypto entrepreneurs was like, “Wow! These people are mostly terrible.” They’re mostly like really terrible. The feel, there's like this huge arbitrage of just as a smart person getting to crypto, don’t be a weird person and you’ll do great.

[00:41:06] JM: It was hard for me, because I would interview these Ethereum people about the, as you called it, the double backflip of trying to get sharding. I was like, “Man! I feel so dumb talking to these people.” They got these brilliant sharding solutions and it's like distributed systems on steroids mixed with microeconomics. I just don't understand it. They’re all smarter than me.”

[00:41:28] HQ: The reality is most of the people who’ve been billing blockchain for long time are astronauts. They’re like these cyberpunk pie-in-the-sky, like Galilean type figures, which is great and you need those people, but they are not a go-to-market people.

[00:41:42] JM: They’re tilting windmills.

[00:41:43] HQ: Yeah, exactly. They are not startup people. Much of what we’ve seen in the last couple years is really as a result of the ICO bubble. We’ve seen a massive influx of high-quality entrepreneurs, and that also accounts a part of the reason why I started working on a company and transitioned into investing was because I saw, “Oh! That arbitrage in large part got filled.” Good entrepreneurs did come into this space and they did start building companies, and now the products are way better than they were two years ago.

I think I'm somebody who probably will eventually end up going back into entrepreneurship at some point, but really when I have an idea that I'm highly convicted about and that I really feel like, “Oh! This thing is awesome and it should exist and I think it’s a great idea.” Now, for me, that bar is higher. It’s not just like, “Oh, hey! Bloomberg for crypto. That should be a thing.” Right now, I see a bunch of great entrepreneurs in crypto and I’m happy to see them there grinding on stuff.

[00:42:35] JM: Maker DAO is cool.

[00:42:37] HQ: Maker DAO is very cool.

[00:42:38] JM: I did a show on that. That was interesting because that was a company where at first I was like, “Oh, wow! This is just as confusing as the sharding double backflip.” But the difference was after beating my head against it for enough time, I kind of got it. I think I still don't completely get it, but like the economic system intuitively felt like it made more sense to me.

I mean, the line is so hard to draw sometimes. There are these – Are there any protocols? Maker DAO, the people seem really smart. The ideas make sense and it has gone to market successfully. Are there any more like shaky dubious cases where you're not exactly sure? Maybe you can’t call them out.

[00:43:26] HQ: Yeah, I don't want to make any particular callouts, but yes. The answer is yes.

[00:43:30] JM: Things that are like on the border between – I mean, I’m trying to put this into the form of a question.

[00:43:36] HQ: Yeah. I mean, you’re familiar with Tether, right?

[00:43:38] JM: Right. Tether. Okay.

[00:43:40] HQ: Yeah. Tether is the world's largest stablecoin. They’ve got over I think $4 billion of outstanding Tethers issued. The whole idea behind Tether is very simple.

[00:43:48] JM: Tether is still growing.

[00:43:49] HQ: Oh, yeah. It's grown. It's grown more than probably any other DeFi product. If you want to call it DeFi. Tether, for those who are not familiar, Tether is literally – Here is how Tether works, okay? Somebody sets up a bank account originally in Puerto Rico. Now, somewhere else, apparently. Basically they put dollars in that bank account and they issue Tethers, and anybody can trade Tethers. When they send Tethers back to the Tether company, they say, "Okay, great. We're going to destroy these Tethers and give you back the dollars."

It's essentially just like some company's balance sheet tokenized that's freely tradable. So there have been tons of scandals of Tether over the last couple of years where, one, like Tether lost their banking relationship at some point. They had like go shopping around for a new one, and that kind of crashed the price a Tether for a little while. Then they were sued by the New York Attorney General's Office for basically Bitfinex, which is the exchange that kind of shadily is connected to Tether. They are like the same directors. They like gave a loan to Tethers in exchange for something, which under collateralized the money that was supposed to be held by the Tether Corporation. The loan went from Tether to Bitfinex. A lot of craziness.

Despite that, it is the most trusted stablecoin in Asia by far. In Asia, people treat Tether as cash. They basically see it as the most trustworthy asset to have on-hand. In the U.S., I mean, the New York Times did this huge hit piece against Tether back in 2017, and pretty much everybody in the U.S. You sort of can't be caught dead holding Tether in the U.S., which kind of shows you the very, very big gulf between what's going on the east and west with respect to crypto.

This is sort of a wider conversation, but, one, most of the capital in crypto, most of the money that actually is chasing these assets; Bitcoin, Ether, all the stuff, it's not coming from the U.S. U.S. is like maybe 20% of all volume. Most of it comes from Asia. That makes sense when you realize that Asia has very tight capital controls all around the world. They have much more demand for U.S. dominated financial assets and they, like us, have stagnating growth and they have a lot of capital chasing not the many good deals.

There's a very big macro picture that also plays into what's going on in crypto that it’s hard to disentangle from the technology. So Tether, despite being probably one of the shadiest companies in crypto, is the largest stablecoin by far and it really shows no sign of being toppled anytime soon.

So at one point, I was very certain that Tether was going to collapse and that it was going to be replaced by something better. I am no longer convinced of that. I think now it's more likely that Tether is going to rule the roost for a while until there is a slow, probably, unceremonious transition. But for the time being, Tether is here to stay. There are more things in this world than in your mind philosophy.

[00:46:33] JM: Right. You've spent some time in China recently, right?

[00:46:37] HQ: I have, yeah.

[00:46:38] JM: Do you have any perspective for how crypto is changing China, or how China is changing crypto?

[00:46:44] HQ: Definitely more China changing crypto, because China is just a powerhouse relative to crypto. I mean, in the eyes of any country, crypto is pretty tiny, except maybe Korea. I would say that the most interesting news that’s come out of China over the last half year is that China is issuing a central bank digital currency, which is sort of their response to Libra, which is Facebook's new digital currency.

A lot of people are really excited about this. A lot of people think this is bullshit. It’s kind of hard to tell what's real and what's not. Except we know for sure this is happening. I suspect that this is likely China's way of trying to address the very, very loud clamors for blockchain in crypto currency to become an important part of Chinese technology strategy.

[00:47:28] JM: Loud clamors.

[00:47:29] HQ: Yes. There’s something like the space race going on right now between the U.S. and China, and can feel it's more on the Chinese side that it is on the U.S. side. But China is –

AI is the big thing. Right? AI is the foremost thing that China is like, “Look, we have to make advances in AI. We have to show that we’re really serious about investment here.”

They've done quite a lot of catch up work in the realm of AI. Blockchain is kind of their second thing. They're looking a blockchain as, “We don’t want to fall behind in what might be a very important pivotal technology.” Of course, they have no idea what they’re talking about.” They don’t really understand what that means, because they think that means corporate blockchains and it means something about the central bank currency.

[00:48:09] JM: You’re talking about the Chinese government.

[00:48:10] HQ: The Chinese government. Yes, absolutely.

[00:48:11] JM: I mean, that's a step ahead of the U.S. government, right?

[00:48:14] HQ: Oh, by far. By far. Yes. I mean, the U.S. government basically doesn't care.

[00:48:17] JM: What about U.S. intelligence agencies?

[00:48:19] HQ: So we know that the U.S. intelligence agencies have done a lot of work trying to deanonymize crypto networks and to try to track what's going on in a lot of these networks. I mean, knowing what we know about like the NSA’s capabilities post-noden, we should not be surprised to know that they’re basically tracking all the Bitcoin flows everywhere in the network and they’re running spy nodes and doing all of these sort stuff, because why wouldn’t they? That's basically all they do.

That said, the U.S. government itself is mostly – I mean, if you saw those, the hearings that they did with the Libra when David Marcus went to Capitol Hill. Mostly they’re interested in blocking Libra. They don't really want this to happen.

[00:48:55] JM: They don’t want Facebook to innovate on its subscription business.

[00:48:58] HQ: Exactly. It's the exact opposite thing they called for when Mark Zuckerbeg came to testify. I think the U.S. government is facing a very different set of tradeoffs than China is. The U.S. government is not trying to compete with China. They know that already had. They're not concerned about – That being said, I do want to give the government there due. They have been relatively open-minded on blockchain regulation and compliance and innovation. They're not shuttering it, which they very much could, and some countries have.

If you look at like France or Japan, there are places where certain concurrency have been banned outright by the government. That's not happening in the U.S. So that's good. But regulations here moves very slowly. It's very hard to get people to create a regularity framework or sandbox where people can safely innovate in. That's driving a lot of the innovation outside of U.S. So if U.S. is okay with that tradeoff, which it seems to be, then okay. That's how it is. But China wants to sit on a different side of the tradeoff.

[00:49:58] JM: So when you're talking about the space race, crypto space race in China's eyes, what kind of investments – Are they making any kind of investment? It is just the digital currency that's an alternative to the Libra, like not really anything interesting.

[00:50:15] HQ: Basically I would say not really anything interesting. I mean, the Chinese government is basically – There's a in crypto, which is blockchain, not Bitcoin, which is a phrase that like everybody who's doing crypto knows that phrase very well.

[00:50:27] JM: Yes. Did we get over that phrase?

[00:50:30] HQ: Oh, no. It's still very much alive.

[00:50:31] JM: Oh my God!

[00:50:32] HQ: Basically China is blocking, not Bitcion. That's their space race. That's what they think is going on. Of course, most of the really sophisticated investors realize, "No. Bitcoin is like – That's the thing that you need to be paying attention to." Bitcoin everything going on this permissionless global platforms. That's what you should be afraid of. That's where the real

space race, where the real place where power is going to move and be exchanged between governments and these networks. That's where that’s going to happen.

I think for the most part, these big investments into what are essentially enterprise blockchains or just like changing the infrastructure of the central bank to be a blockchain instead of whatever other kind of databases it is. To me, that is completely immaterial. That’s just marketing essentially. Bu China is investing a lot into that for better or for worse, and they are partnering with a lot of the largest companies and institutions within China to be direct recipients of access to their central bank digital currency.

I suspect that if nothing else, that is going to galvanize other central banks to follow suit if China does that and does it successfully. That has a lot of knock on effects for monetary policy and for traditional payments and how that’s going to change over time. The influence that’s going to have on crypto [inaudible 00:51:47] crypto, is pretty minor. It might mean that, “Okay. Now maybe we can tokenize Yuan using the central bank digital currency, like do a cross-train swap.” That’s not really anything to write home about. I’d say for the most part, unless these central bank digital currency ledgers actually enables smart contracts, which I suspect most of them won't. That’s not really in the plans. I think they basically just fundamentally don't understand what is the value proposition of these new blocking networks.

[SPONSOR MESSAGE]

[00:52:25] JM: Feature flagging makes it easy for your team to quickly change the way that your product works, and CloudBees Rollout lets you manage feature flags easily. When you have a solution to manage feature flags at scale, you’re empowered to continuously and intelligently rollout changes as soon as they are code complete on any platform, even mobile. You can decouple development from code release for a real-time change control. You can rollback only the changes that you don’t want, or keep them around.

You can toggle features. You can use multi-varied flags for A-B testing and you can remove misbehaving features with a kill switch. All of these is part of the feature flag platform that is CloudBeess Rollout.

[INTERVIEW CONTINUED]

[00:53:50] JM: Coming back to your article, what we're talking about before the podcasts is that we really don't know a whole lot about how to take a crypto startup to market. I mean, we have some historical examples like Coinbase, or I guess Maker DAO, or I guess Ethereum, or the CryptoKitties company, and then I heard Fort on the a16z show yesterday, a16z podcast. So, yeah. Do we know anything about how to go-to-market as a crypto company?

[00:54:27] HQ: The answer is no, not really. Basically, we have a lot of examples of what doesn't work, and we have a few examples kind of what does work, but they're not particularly replicable. The exception to that is in – You mentioned Coinbase. Coinbase is very replicable. There literally are Coinbases in different parts the world that run the same business, their exchanges or their wallets.

Those types of picks and shovels type services we understand pretty well how to run. We know what the playbook is for a lot of these. Of course, there are things like lending and derivative exchanges for which if you look at retail Forex exchanges, that is a good playbook for what it looks like to do a lot of these retail, speculator-focused companies that are offering financial services.

For the real deep crypto stuff, the answer is that we don't know. We're sort of making it up as we go, and the reality is that the terrain is changing so rapidly that if you copy Ethereum, you're making a fundamental mistake. The crypto market, the people in this space, the average consumer you'll be dealing with is different. They have different beliefs. They have different understandings of how to use technology. They have different products available to them. Everything is changing too rapidly for us to have a really congeal playbook. So the answer is that there are bits and pieces you pull from each of them. But for the most part, it's kind of up to you and your business to figure out how exactly you need to go market.

[00:55:48] JM: Give me a pulse check on the Bitcoin and the Ethereum communities.

[00:55:53] HQ: Everybody is still alive. They're all doing well. They still hate each other for the most part. Bitcoin, I think this probably betrays my allegiances as not really hardcore Bitcoiner, but I'd say for the most part, Bitcoin is still Bitcoin. Not a whole lot has changed. There're always a few technological innovations in the pipeline, like Mast, like Dandelions, things like that.

[00:56:12] JM: Lightning network is there, just people don't really use it.

[00:56:13] HQ: Lightning network exists. Yeah, it's small. It's tiny. I mean, people will tell you, "Well, they haven't increased the debt in the ceiling or whatever." The reality is that like there is not a ton of demand using lighting yet, and I sort of spec that's not likely to change in a dramatic way even if they onboard more people, because the reality is it's just not – It's not a great yield producing thing to put money into.

[00:56:32] JM: People are cool with Venmo right now.

[00:56:34] HQ: I mean, yeah. People here are cool with Venmo, and people don't want to pay each other in Bitcoin. That's just not the way that they think about paying people. I think –

[00:56:44] JM: Buenos Aires, why wouldn't they use the lighting network to transfer money to each other?

[00:56:49] HQ: They might also use Dai, they might also use Dai. They might also use U.S. dollars. They might also use other currencies. The reality is that there a lot of alternatives in most of the circumstances. Bitcoin is not the only game in town, and they might use local Bitcoins. Maybe they don't need lighting. So the reality is there are many ways to engage.

[00:57:07] JM: It's like we got the systems for the throughput and the demand for the throughput is not there.

[00:57:12] HQ: The other thing is that it's nontrivial to get set up and lightning. You have to first create a channel and open it up and get liquidity to your thing. The software is not fully baked yet. So there are some barriers that probably will get easier overtime, but the reality is like it's not as straightforward as just like having a phone number and then having somebody send you money, which is what it's like for a lot of more traditional fintech companies that are certain to compete in the same category. So that's Bitcoin land.

In Ethereum land, I think there're a lot of excitement around Ethereum 2.0, which is going to be the new version of Ethereum, which is much more scalable. It's sharded. It's all the stuff we talked about. All the stuff you need a PhD to understand. That stuff is coming down the pipeline. But the reality is everybody who's honest will tell you it's really two years plus away. There's going to be like V0, which is not functional, which doesn't have smart contracts and basically is not what was promised on the 10.

They're doing sort of iterative rollout where it's like, "Okay. First is we're just going to have a network that is consensus. Then we're going to have a network where you can send people money, but there're no contracts. Then you can put data on it. Then finally you will actually have full smart contracts and will be the thing that you thought you wanted in the first place." That is probably 2+ years away.

So that means that there's also a window for a lot of other competitors where much more scalable smart contract platforms that are planning to launch within the next year or two. So there're things like Telegram. Telegram has a – For those who are not familiar, Telegram is like a really big end-to-end encrypted or supposedly end-to-end encrypted messaging network. It's kind of like Facebook Messenger. It's got like 250 million users or something like that. They're launching Telegram coin called – Their network is called Ton, and that will probably be launching sometime within the next few months is my understanding.

Then we've got the Libra supposedly launching next year, but that seems optimistic. I doubt that's going to happen. A lot of other mega lunches that are similar competitors with Ethereum. Kind of what that means is that there's a lot of innovation going on in Ethereum, but there are these marauders coming over the hill and they're reeling their cans behind them and we'll see whether Ethereum can hold down the fork.

[00:59:17] JM: I made a comment about execution risk in the self-driving car and so on. Worries about execution risk on the Ethereum front? Do we have any reason to be concerned that smart contracts may be much harder to do than we think?

[00:59:31] HQ: I think we already know that smart contracts are harder than you think. The reality is all these stuff is messy. Everything is a hack on top of a hack. That's how it's good to be.

[00:59:42] JM: That's how the Internet is.

[00:59:43] HQ: That's how the Internet is. The Internet was slowly, slowly taking all of the thorns and splinters that we shoved in there in the first place out one-by-one. Did you see this thing? What is it? Simjacker? Simjacking?

[00:59:55] JM: I mean, just the idea that you're sim – I don't know what –

[00:59:59] HQ: There was this attack that was incurred recently where basically attackers can send specially formed SMS messages to your phone that will actually run code on your sim card. It turns out, your sim card – Guess what? Is a computer. It can run arbitrary code and it call out custom domains, and it turns out that people can basically take over your phone and have it perform arbitrary commands through this attack.

So it's believed that basically this attack was like there is some suite of software that was almost certainly made by nation states to target individuals for this type of attack. That's like potentially a large swath of phones that are vulnerable to this, because they use sim cards. That's all software. That's everything. I don't think blockchains are an exception to that, and smart contracts are certainly not.

The most we can expect out of these things is that they're going to keep getting better quickly. What we want to see out of blockchains is not they're great perfect systems that never break and kind of are perfectly decentralized and perfectly functional all the time and great. That's a great aspiration to have, but we're not going to hit it, and it's important to realize that.

What we want is just to keep growing and keep getting better and to have that Moore's law like trajectory that the internet had. That is what's going to make crypto into a sustainable innovation. If we hit a wall and we're just like, "Oh, shit! This is basically as much as we can do." That's what worries me more than that Eth too is going to be bungled when it finally comes to market. Of course, it's going to be bungled. I mean, it's hard. It's crazy. It's rocket science.

[01:01:25] JM: We hit a wall with.

[01:01:27] HQ: I think it's possible that we might hit a wall with just like fundamental constraints on consensus and replication. It may well be that the idea of sending all these peer-to-peer messages and everybody agreeing on the state, there's fundamental physical limitations on how much compute you can get through a system like that. If that's true, maybe would top out at something like a thousand transactions per second or 10,000 transactions per second. If you want to pass that and really onboard more commerce on to crypto, it's just basically impossible.

Part of the dream of layer two is that that can be circumvented through these other mechanics, but they're really high-friction, they're really hard to make systems that paper over those boundaries and it might just be that like the best UX you can get in crypto is shitting. If that's truth, if can never get a good UX in crypto, that worries me.

[01:02:18] JM: Let's close off with some startup advice. You've been in the valley for a while. There is this dispute in the world of startups over the extent to which a startup idea should be predetermined. The extent to which you should say, "This is my mission. We're building a rocket to Mars to make human beings sustainable," versus a pivot-heavy strategy or a neutral pivot open strategy. Do you have any general advice when it comes to being strongly deterministic when it comes to your startup idea?

[01:02:58] HQ: I'm pretty open to the idea that being pivot friendly is a good idea early on. Ultimately, you're not going to know whether a startup idea is good before the world tells you something about it, and you're certainly not going to learn what the difference between a good idea and a bad idea or whether or not you can achieve product market fit just sitting in your bedroom and whiteboarding, right?

At the end of day, it is through your interactions with potential customers/users/whatever that you are going to figure out is this an idea that has legs or not. I mean, ideally, the dream is that you already know who your first customer is before you even start working on a startup. Those are the juiciest startups to be building when you are just certainly like, “Look, we just have to build this, and we’re definitely going to get customer.”

If you’re not in that situation, a lot of building a startup I think is more about listening to what the world is telling you and to what your customers are telling you than it is about you declaring what your idea is and what you're going to do. So I think, in general, entrepreneurs would be better served by lessening their conviction in a particular idea so much as having conviction in exploring an idea, which I think is different.

[01:04:07] JM: Haseeb Qureshi, thanks for coming back on Software Engineering Daily.

[01:04:10] HQ: Thanks for having me as always.

[END OF INTERVIEW]

[01:04:20] JM: As a programmer, you think an object. With MongoDB, so does your database. MongoDB is the most popular document-based database built for modern application developers and the cloud area. Millions of developers use MongoDB to power the world's most innovative products and services, from crypto currency, to online gaming, IoT and more. Try Mongo DB today with Atlas, the global cloud database service that runs on AWS, Azure and Google Cloud. Configure, deploy and connect to your database in just a few minutes. Check it out at mongodb.com/atlas. That's mongodb.com/atlas.

Thank you to MongoDB for being a sponsor of Software Engineering Daily.

[END]