EPISODE 531

[INTRODUCTION]

[0:00:00.3] JM: Dogecoin was started in 2013 as a joke. Jackson Palmer forked Bitcoin and created his cryptocurrency as a playoff of the doge meme. The currency became popular as a means of Reddit users tipping each other.

If I made a comment on Reddit that you liked, you might send me some doge coin. This use case allowed people to share the idea of Dogecoin virally and Dogecoin became valuable, even though the currency did not have any technical properties that made is significantly better than Bitcoin.

As Dogecoin became popular, an experienced internet scam artist took notice and started a Dogecoin exchange called Moolah. Moolah was used to steal money from its customers and investors and the CEO was arrested.

Jackson Palmer was not involved in the scheme, but it soured his feelings about Dogecoin and the entire Bitcoin space. His coin, which had been created as a joke had been hijacked and repurposed as a weapon to steal money.

Jackson left the Dogecoin community in 2015 to focus on other things. As Bitcoin entered the mainstream conversation, Jackson has been pulled back into the world of cryptocurrency. Jackson's YouTube channel has over 20,000 subscribers who tune in to learn about consensus protocols, new tokens and cryptocurrency news.

In today's episode, Jackson and I discuss his experiences with Dogecoin and how that compares with the scams around low-quality ICOs that are pulling retail investors today. We also discuss more positive things such as proof of stake and newer consensus protocols.

If you're looking for an internship, apply to the Software Engineering Daily internship at softwaredaily.com/jobs. If you're looking to recruit engineers, you can post jobs for your

company there as well. It's completely free to post jobs and to apply and we're hoping to find interns to contribute to the Software Daily open source project.

If you want to see what we're building, you can go to softwaredaily.com, or check out our apps in the iOS or Android app store. They have all of our episodes with recommendations and related links and much more material.

Also, meetups for Software Engineering Daily are being planned. Go to softwareengineeringdaily.com/meetup if you want to register for an upcoming meetup. In March, I'll be visiting Datadog in New York and HubSpot in Boston. In April, I'll be at TeleSign in LA. I hope to see you there.

[SPONSOR MESSAGE]

[0:02:34.7] 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.

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 consensus 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 CONTINUED]

[0:03:51.3] JM: Jackson Palmer, you are the founder of Dogecoin. You're a product manager in the Bay area. Welcome to Software Engineering Daily.

[0:03:58.8] JP: Yeah, absolutely. Thanks for having me on, Jeff.

[0:04:01.5] JM: You started Dogecoin four years ago and it took off despite being started as a joke. Why did people buy Dogecoin?

[0:04:12.1] JP: Yeah, it's funny. A lot of people ask me in the early days, why do I think that it took off and had that virality that it did? I think an often overlooked part of the equation was that people weren't actually buying it. I think, early on it was very easy to mine, because it was using S script algorithm, which at that point in time was still easily minable on home GPUs. Anybody with a gaming rig could point their computer at it and mine some.

In addition to that, the most usage was happening on Reddit actually, where a tipbot had been built by a community member called Doge tipbot. Through simple comments, took those tipbot tip this person a 100 Dogecoin, you could send anybody on the platform on Reddit some Dogecoin, whether it was because it's something they posted, or comment they made without that user requiring a wallet that they had themselves.

There was this in-build virality there of pay it forward, pay it forward happening on Reddit. I think that's really what made it as successful as it was, and not necessarily people going and buying it with their own money.

[0:05:21.4] JM: That was actually novel technology at the time.

[0:05:23.8] JP: It was. I think it still is. I think that was a few years now where tipbots where extremely popular. They seem to have tape it off a little bit. There was even some startups in the space that tried to do tipping since – I think they faded away most because of transaction fees on these networks getting too high for the stuff to work properly. Yeah, it was novel for the 2013.

[0:05:43.1] JM: What were the other non-Bitcoin cryptocurrencies in 2013?

[0:05:50.2] JP: Yeah. Actually what inspired the creation of Dogecoin was my interest in Litecoin and then subsequently Fetacoin. Fetacoin was a derivative of Litecoin itself, but it had – it was based in the UK and it was a very community-driven and local community-driven, which I liked and they had a passionate community of people involved. When Dogecoin extended beyond the joke, that's where I was drawing many inspiration from.

[0:06:19.7] JM: People who start learning about cryptocurrencies, especially today, they often talk about going down the rabbit hole, which is a term that describes getting so infatuated with technology that you stop doing anything, except reading about cryptocurrencies and consuming information about it. How intrigued were you by it in 2013? Did you go down the rabbit hole, or was this just a part-time fascination?

[0:06:49.1] JP: Yeah, that's a good question. I initially didn't go down the rabbit hole, because I was skeptical of all the stuff. Dogecoin, when I tweet it, I'm going to Dogecoin. It's the next big thing. That was a joke and it was very obviously a jab at the flurry of alternatives to Bitcoin that were hitting the market.

I didn't want to go down the rabbit hole, because I've seen people do that. The interesting thing about that, the analogy of going down the rabbit hole is I think a lot of the addiction, if you will, is driven by speculative trading and the price rather than actual infatuation with the technology. I didn't want to become a crazed day trader overnight and so I try to avoid it.

As I got more and more involved in Dogecoin early on and eventually took on core development for it, I obviously needed to go down that rabbit hole from a technology standpoint and understand how Bitcoin works.

[0:07:44.3] JM: In 2015, you left the Dogecoin community. This was when there were scams and thefts associated with the currency. Today in 2018, there are many more scams and thefts involved in many more currencies. Did you realize then that what you were seeing with Dogecoin was just a small preview of what was to come in terms of all these scamming?

[0:08:12.3] JP: No. I absolutely couldn't have predicted that it would grow to the level that it has now. I saw Dogecoin as the pinnacle of mania back then. I left in 2015 after the whole industry had been hit by a lot of scams and consumer option was reaching a low and interest was

dwindling from venture funds. I was like, “I think this spot is over.” I really did not anticipate the resurgence that has happened. There are definitely parallels though, and so I think Dogecoin is a historical case study is very important and useful, as a mirror to shine back on what’s happening right now.

[0:08:54.2] JM: That historical importance, one way to describe that is as far as I could tell, it seems like Dogecoin was the first coin to get hijacked, where someone from outside of the core team took advantage of the currency and the currency’s community.

[0:09:12.3] JP: Correct.

[0:09:12.8] JM: Okay. You agree. Good. This happened more recently with pumping and dumping of all kinds of currencies. You could start a currency and not have a conspiracy around it. Maybe a pump and dump group just takes it on and pump and dumps it for you and you don’t even have to be explicitly complicit.

It looks like this might’ve happened with XRP, for example. Is there a way to prevent that – if you start a currency, is there a way to prevent somebody from hijacking your currency and pumping and dumping it?

[0:09:49.3] JP: Yeah, not really. I think it’s the virtue of A, it being open source and B, having it being a currency or trying to be a currency. I think that the interesting thing with Bitcoin and all of its derivatives are that they’re really the first open source projects, which have financial incentives built in. Which I think for an engineer is a very interesting problem, because if you look at previously successful open source protocols such as Bittorrent, Tor, or even something like Linux foundation and Linux kernel, none of these open source projects had a financial element baked in.

Incentives were ultimately just kind of, let’s build good software and if people like it, then it will become popular. With cryptocurrency, there is like an inherent value obviously associated with that code. Because it is open, there’s nothing stopping anybody coming in and co-opting the community around that.

Obviously it's way easier to co-opt to community when you don't have to even fork it and write that a code. You can simply pay that community or hide that community up around speculative pricing process.

[0:11:00.4] JM: In this community, there are these people who they start a project and it's like we're going to decentralize X and it's going to be beautiful and the internet is the way that governance should happen and we shouldn't have any like traditional governments and whatnot. They do an ICO and they make a ton of money.

I mean, when I've talked to some of these people, there seems to be a conflict where I think they know deep down that the reason people are buying their ICO is not because of the fundamental value, the fundamental promise of their decentralized utopia. It's more the speculative nature of it. Do any of these people that you've talked to that have done these ICOs, do they feel morally conflicted, or do they even have trouble processing it morally?

Because they find themselves in this position where they're tremendously rich and their project has not really gone anywhere and been used for anything. Then they look inside themselves and they're like, "Hmm. Now I don't feel so motivated to decentralize the world. I wonder why that is."

[0:12:10.1] JP: Yeah. I think these people exist in almost a state of blissful ignorance. I think it takes a certain type of person and personality to be able to maintain that façade. You look at a lot of these projects, things that are like, we're putting the dental industry on the blockchain, or a lot of these things that are doing enterprise plays with these app tokens.

Why are thousands of consumers all across the world buying these things? Like obviously not to actually use a platform if it ever is built, but mostly so they can flip the thing for some speculative profit in the future. The funny thing is if you talk to any of the people involved in this project and I do talk to them all the time. I think, whether it's simply to maintain their legal position or whatever, I think that they're very proficient in maintaining that façade and saying, "Oh, no, no. The people are actually going to use this thing."

It's very strange and I think it is a conflict of interest, because the developers who find themselves in this position – well, that's if they even are developers. When they find themselves in this position of having a whole lot of money, they tend to focus on maintaining that wealth, rather than actually switching into developing the software.

I think what's even worse is we've seen a pattern of teams doing this whole thing with the ICO, but then only after raising that money then going and hiring developers, which I think is obviously the wrong way, or just kind of stop.

[0:13:35.1] JM: Yes, indeed. There are so many opportunities for people with notoriety to help with the pump, like you see with John McAfee or Paris Hilton. Have you been tempted at all, because I'm sure you have the opportunity to do that. If you wanted to, you could do it. It seems like you have resisted that temptation this far.

[0:13:56.0] JP: Yeah, absolutely. I definitely try to resist that. I believe in maintaining your own integrity as a person, because when all this is set and done, you're still going to have to have your reputation to bank on.

I've obviously been solicited by a lot of these ICOs, they send me an e-mail. They say, "Hey, we'll pay you all these tokens if you'll do a video, or if you'll tweet about us." I just cut them off right there and don't want to be involved, because A, I don't want to be seen as a promoter of what might be deemed an illegal security in the future. Also, I just don't see a lot of merit in most of the technology being marketed or promoted right now, if there is any technology.

A lot of these stuff is very shallow. You go to their website and their whitepaper's being written by somebody who's obviously a non-academic. Obviously, somebody who is maybe done some online marketing in the past and there's just not a lot of substance. It's very rare. I keep out of that and I try to just remain objective and call things out based on their actual merit, if I see it which is rare. Rather than ever considering taking promotional money.

[0:15:10.0] JM: Yeah. Or the whitepaper is just completely plagiarized. When you left in 2015, when you left the Dogepoint community that was around the time Ethereum was coming out. Did you pay close attention to Ethereum at the time, or had you relegated cryptocurrencies entirely to some small margin of your attention?

[0:15:31.8] JP: Yeah. I'd been during 2014 going through a lot of events and being around people, like Vitalic a lot. To be frank, I thought it was vaporware. I didn't think that this thing would actually ship. This was prior to them doing that inquiry.

[0:15:44.4] JM: That makes two of us.

[0:15:45.0] JP: Yeah. This was prior than doing the crowd sale. I think I had a bunch of friends here in San Francisco we have sitting around, they're like, "We're putting some money at Bitcoin into the Ethereum." Token sale or crowd sale was like, "That's never going to launch."

What I didn't anticipate was that they would take the bulk of that crowd sale and just spin up multiple engineering teams and still like throw it in the wall and see what sticks, right? That's eventually how Ethereum got launched is they placed a lot of bets with multiple engineering teams and they released the one working client, or the best working client. I have to give them credit for actually shipping something, because I just didn't see it happening.

Obviously, it stings a little bit when I see these friends that I was sitting around with now who are like multi-millionaires because of that decision. At the same time, I think what they did ship with Ethereum is very much a beta product if that – I think we're already stopping to see some of the issues with the scaling, but just the fact that Ethereum's had to fast follow with these much more complex protocols, like Casper and plasma and I think speaks to the complexity of the problem and how the initial build may not be sufficient for the scaling to where it need to be.

[SPONSOR MESSAGE]

[0:17:07.4] JM: The Casper mattress was designed by an in-house team of engineers that spent thousands of hours developing the mattress. As a software engineer, you know what kind of development and dedication it takes to build a great product.

The result is an exceptional product and when you put in the amount of work and effort that went into the Casper mattress, you get something that you'd use and recommend to your

friends. You deserve an exceptional night's rest yourself, so that you can continue building great software.

Casper combines supportive memory foams for a sleep surface that's got just the right sync and just the right bounce. Plus, its breathable design slips cool to help you regulate your temperature through the night. Stay cool people. Stay cool.

Buying Casper mattress is completely risk-free. Casper offers free delivery and free returns with a 100-night home trial. If you don't love it, they'll pick it up and give you a full refund. Like many of the software services that we have covered on Software Engineering Daily, they are great with refunds.

Casper understands the importance of truly sleeping on a mattress before you commit, especially considering that you're going to spend a third of your life on that mattress. Amazon and Google reviews consistently rank Casper as a favorite mattress. Try it out. Get a good night's rest and upvote it yourself today.

As a special offer to Software Engineering Daily listeners, get $50 towards select mattress purchases by visiting casper.com/sedaily and using the code SEDAILY at check out, you'll get the select mattress purchases. If you go to casper.com/sedaily and enter the code SEDAILy at check out.

Thank you, Casper.

[INTERVIEW CONTINUED]

[0:19:13.5] JM: What I didn't realize about Ethereum, the biggest thing that I didn't realize about Ethereum is you look at the morally conflicted, technologically inept ICO pumping numbers that we just talked about. If you were to create the complete opposite of that type of person, that would be Vitalic.

[0:19:30.7] JP: True.

[0:19:32.5] JM: Vitalic is just this guy who's just brilliant and he seems to have a very clear and kind moral compass. His pace of work has never slowed down throughout any of these. It almost seems like he was prepared to rise to the occasion, which is just it almost incredible. I have no idea how that guy manages his life. He lives a crazy life, but the project moves forward and he seems like he's present and he seems like he's calm all the time.

It's just like, you could not imagine a better leader of this type of project. When I compare that to other projects I've seen, it's just like nothing even comes close to the leadership quality. That was probably hard to recognize at the time. Or I don't know, it sounds like you met him in 2014, so maybe you saw the light.

[0:20:16.9] JP: No. I think it was always obvious that he has a spark that others may not have. I'm glad that align with his – you mentioned his claim, but I think he does have a good moral compass, which is something that is honestly hard to find in a crypto space. I think there is a lot of different incentives and people have agendas and he doesn't seem to, which is pretty good.

I think the challenge is going to be shiny object syndrome with him and that team. I think, there's obviously a lot of good developers working on it, but I think – what they need to make sure happens is that the core protocol itself gets a lot of love before they move on to something else.

Underneath all of that, you know I'm a product manager, so I tend to come from these things as before I come up with a solution, let's talk about the user problem that's being solved. I think that's still a huge issue with Ethereum and that outside of ICOs and crypto kitties, which I would say is just another form of ICO in a way. It's all the statements, very linked to speculation.

The reason a lot of use happening of the Ethereum platform. Again, I really think the right direction for them would be to look at what's the actual user problem we're solving? Is it peer-to-peer commerce? Is it some novel uses smart contracts that solves a real bulk problem? Then go from there, rather than inventing protocols which branch off in a million different directions, that are self-serving in meta in a way, than instead of focusing on a core issue.

Which I hope Vitalic does, because I think Vitalic does seem to have a pretty strong moral compass. He does seem to stand for social justice and that kind of stuff. I would like to see him

focus on things that actually contribute back to society, instead of just making the people who've done ICOs richer and richer and richer.

[0:22:13.1] JM: Have you seen anything that resembles a production quality deployment of a smart contract that people can make practical everyday use of, not counting crypto kitties?

[0:22:27.3] JP: No, I haven't. I honestly haven't. I think a lot of these things the solutions – either solutions and such of a problem, which is what often the protocols are. Or in the case of these businesses that are spinning up around smart contracts, they seem to be shoe-horning the idea of decentralization into an existing market that might not need it.

I think it's very important when somebody says, "Hey, we need to do Airbnb on the blockchain, or Uber on the blockchain." I think it's always good to go and look at the products, like Uber or Airbnb and say, they're really having a problem that requires immutable sensorship-resistant database technology essentially, or execution of arbitrary code.

My opinion tends to lean towards not there. I think that people have this and they're bandwagoning right now with a lot of the stuff. Yeah, it's a slippery slope and I think we have – we're in pig mania right now. People saying, it's blockchain for X.

[0:23:24.7] JM: After you stepped away and unplugged from the blockchain community, what brought you back?

[0:23:29.9] JP: When I stepped away in 2015, through 2015 and 2016, I was still working on decentralized technology and tech in general. I released a few work and so side projects and was focusing pretty heavily on how we decentralize social media, which I still think is an important thing just to – not in terms of full decentralization, but just from a data sovereignty and owning your own identity landscape is still important.

I was doing that for a lot of 2015 and 2016 in my spare time. Even released this prototype of social network. Then I got really into this other open source project called Mastodon, which is a federated social network platform.

In early 2017, obviously I was still keeping my ears to the ground with the space, but what actually triggered it is that when the Ethereum price spiked overnight, or over the space of a few weeks, I was in an Uber here in San Francisco by share and one of the drivers was talking about Ethereum.

I was like, the fact that it started weaving its way into every day conversations pricked my ears up. I honestly got flashbacks to 2013 and 2014 when the whole Dogecoin craze was happening. I was like, "Oh, it's happening again. Who knows at what scale?"

That's what brought me back in. I came back and I didn't have any intention of starting any new project, but more just taking my experiences and helping share knowledge about those experiences and come at this stuff from a viewpoint of, "Hey, we've seen this stuff before. Here is how you can protect yourself and here is what you should be focusing on."

Yeah, I started doing my YouTube channel, which is really focused on educational materials and deep-dives into the technology, because I don't think there's enough people doing that. I think most of them at media or outlets and most of the YouTube channels you'll watch will be focusing on what coin is going to pump in the next week.

[0:25:35.2] JM: Indeed. I have found your YouTube material pretty helpful. What piece of advice do you find yourself giving most frequently to people who want to invest in this space?

[0:25:49.4] JP: Yeah. I think honestly, the biggest investment you can make is in yourself in terms of getting into the space. What I mean by that is rather than investing money, I think the best investment you can make is to go and educate yourself about how the stuff works and how potential applications of it, because the people that are really going to succeed in the long-term. I think bubbles come and go, and I have no qualms in saying we're in a bubble right now.

I think the people that are successful are the people that build legitimate businesses and products on top of underlying novel technologies. The people that are going to still be standing in the next five to 10 years are the people who have done the research and done their homework over the next 12 to 18 months.

Then started working on businesses and products that actually solve real-world user problem with the technology that blockchain and decentralization office. Rather than the people that just pour a whole bunch of money into it.

Sure, those people might make money and I should preface that this isn't financial advice obviously. Contact a national financial adviser, but I just think the long play in the space is understanding the technology, so that if you're an engineer, in 12 months when you're working on your next product you might think, "Hmm. There's actually a way that this new technology can help us get to market faster, or in a unique way."

Rather than taking it from – if I'm just going to buy it upright, now I'll be rich. Reason being that I tend to think of these tokens and these cryptocurrencies as companies. Just like in the early internet days, those companies are leapfrog by people who take the underlying concept via the internet back then and do them one better.

I have no doubt that cryptocurrency is like Bitcoin and Ethereum and these things. Or just the early players. They're going to be like the MySpace, as in the Friendsters of cryptocurrency. Because it's so open – because there is nothing that makes these technology different from other technology regardless of how hard it is to understand.

I think that's important for engineers to understand, this is not magical voodoo magic. This is just technology. Because of that, somebody is going to come out and release the Facebook and the Snapchat of the crypto space, and essentially leapfrog Bitcoin, which would be the updated technology.

[0:28:18.1] JM: I totally agree with everything you said. Just to start with the aspect of this just being yet another technology, in computer science, if you study computer science, you study software engineering outside of the university. Regardless, you learn about backend. You learn about frontend, you learn about databases, you learn about restful.

What's intimidating about Bitcoin or other cryptocurrencies I is this whole other stack ad it's – You go over there and you're like, "Oh, my god. It's like almost none of my –" I mean, certain

computer science fundaments certainly translate, but it's you're very much in a blue ocean and you're without a boat and you really have to assemble your boat.

That takes some intellectual effort. I'm still having trouble with it. There's still so much that I really have trouble grasping. I know that it's nice basically do this full-time. I just get to interview people and study the stuff as much as I want. It's still really hard for me. I completely agree that investing in the knowledge is the right way to go about it.

I would also add that that's hard to do, but it's also worth doing and it's going to be valuable, even over a five to 10-year time horizon, because it's a collection of fundamental breakthroughs. Why don't you put a finer point on that? What is the fundamental breakthrough? Because there are these people who are just like, "It's a fad. It's a bubble." Even very smart engineers.

I was talking to somebody at KubeCon, somebody who is like a Kubernetes core contributor and he's just like, "It's the fad." I'm like, "No, no, no, no. This is a core important technology." They just don't get it. What would you say to those people?

[0:29:56.8] JP: Yeah. I think it's not a matter of not getting it. I think what's happening here is a good similarity I would say is with machine learning and AI. I think that if you look at blockchain – Let's start with AI. If you look at AI and neural networks and all of these stuff that it's kind of also having a gold rush now in computer science; these are not new concepts. These are neural nets have been around for many, many years.

The technology and underlying principles that make up technology such as Tensorflow and other machine learning platforms are concepts that – there's a lot of prior out. All that solutions, like Tensorflow and any of these other machine learning frameworks provide is a way of bundling that to get those concepts together in a simpler to use framework and providing some example use cases, if it's image classification, or if it's NLP or something like that.

Now, I think blockchain you can draw a direct similarity to. The blockchain isn't a completely technology either. Blockchain is based on a lot of cryptographic fundamentals that have been around for 20, 30, if not 40 years. All that Bitcoin did was just like Tensorflow, it brought that stuff

together in a framework. It brought multiple disparate concepts such as hashing proof of work, distributed consensus together in a way that it was represented and tangible.

It provided a framework for how to use those concepts together to achieve a use case, which peer-to-peer cache. I think people shouldn't attack it from that standpoint. I think if you think about it that way, it becomes a lot less daunting as a thing, because it's not just something that popped up on the scene yesterday and all of a sudden, you're redundant as an engineer because you don't understand it. No, no, no. I think it's a skill that you can learn. Just like machine learning, it's learnable. Don't think that it's something that is impossible to ever understand.

[0:31:57.9] JM: To take your other point about the Uber driver, I have had several conversations with Uber drivers about their decentralization project, or their Bitcoin investments. I think this is the modern equivalent of the shoe shiner. You're not supposed to invest when your shoe shiner is talking about – This was something that I used to say in the wake of 1920s market crash. You don't invest when your shoe shiner is talking about a stock, because that means that there's no secret information left. It's made it to the shoe shiners.

The market is fully valued, or overvalued. You captured this in an article that you wrote called My Joke Cryptocurrency hit 2 billion dollars and something is very wrong. This was something you wrote a few months ago. I thought you captured the moment quite well in that article. This was just before the reason precipitous drop that probably was not the bottom, but what were you trying to capture in that article?

[0:32:58.1] JP: Yeah. I was trying to capture definitely this kind of hyperbole that exists around blockchain. The subsequent speculation and money coming in that has resulted from it. I think that back in 2013, even though there was a mania going on, I think a larger number of people in the space wanted to understand the underlying technology.

They had a vision. They were trying to solve particular use cases. Back then, it's also important to remember that things like Venmo and Apple Pay, they just didn't exist, or they weren't as successful as they are now. Solving peer-to-peer payments was actually a really – a right market ready for disruption back in 2013.

I think over the years, the whole notion of blockchain has gotten swept up in this marketing pitch almost. People say blockchain, everybody's, "Ooh. I don't understand it, but it's this magical thing, right? Only geniuses get it." As a result, I think we've just – everybody spending their time focusing on the markets rather than focusing on the actual underlying technology and whether it solves a problem.

I think Bitcoin had a really strong chance of solving the problem back then. I think now, the switching cost is a lot higher for end users, because they have solutions like Venmo and Apple Pay, which would be extremely low friction. Why would I go and use something that's more expensive and slower, right?

I think the shift in focus over to these hyperbolic statements about how blockchains, like the creation of the internet in terms of its importance and technological advancement are it's going to change the way we do everything. I think these hyperbolic statements only serve to pump the market up further, which is going to detract from and distract everybody from actually discovering real use cases of this stuff.

When the bubble ultimately bursts, my concern is that people will just say, "Oh, well. That thing was just – there was no substance to that," and they'll move on. I think ultimately, that could do damage to the industry. Again, what I'm trying to talk about is I think the developers need to spend more time developing and less time being day traders.

[0:35:11.1] JM: Indeed. Well, let's talk about some of the projects that you've covered in your YouTube channel and the other things you're excited about. What are the projects that you're most excited about? What are the interesting technical breakthroughs that are top of mind right now?

[0:35:26.3] JP: Yeah, absolutely. For me, the things that are most interesting are again, the things that hawk back to that initial value prop of providing peer-to-peer cache network. I think we never really nailed that. I don't see why we're moving – we're like raising a thousand miles ahead of ourselves.

Technology such as there's a protocol called the spectre protocol, the subsequent implementation or plan for implementation and that called phantom. This is from a team out of Israel and it basically takes Bitcoin blockchain model, but scales it using directed and simply graphs to basically allow a parallel finding of blockchains, which is very cool.

I'm really interested in these technologies that take the existing model and evolve to something where we could actually maybe see a version of Bitcoin that is fast and cheap to use and can run on people's funds. Another one that I think is important to look at is that recent proposal called Mimblewimble as a implementation on Github called Grin.

Again, a similar thing where it takes Bitcoin and it scales it using some pretty novel cryptographic work. Again, it's not new technology, but it's just taking prior at and basically bundling it together in an efficient way. Those are the projects I'm really interested in. I think that the things that are really down low with the infrastructure level and rethink things, rather than it's blockchain for X, because I think those – as we saw with Uber, I think remembers a couple years ago, there was the on-demand economy where everybody was doing something Uber for whatever. I think that dries up pretty quickly and I think we'll see this similar behavior in the crypto space, especially if the underlying protocols can't scale.

[SPONSOR MESSAGE]

[0:37:18.1] JM: When you're building an application, you needed to be fast, secure and always evolving. With Kubernetes engine on Google Cloud platform, developers can deploy fully managed containerized apps quickly and easily. Google has been running production workloads in containers for over 15 years. Google builds the best of what they learn into Kubernetes, which is the industry-leading, open source container orchestrator.

Kubernetes engine combines automatic scaling, updates and reliable self-healing infrastructure with open source flexibility to cut down development cycles and speed up time to market. To learn more about Kubernetes engine, visit g.co/getgke. That's g.co/G-E-T-G-K-E. G.co/getgke.

Thanks to Google Cloud for sponsoring Software Engineering Daily.

[INTERVIEW CONTINUED]

[0:38:23.2] JM: The first thing you mentioned, spectre with this parallel mining of blockchains. What is parallel? Can you describe that parallelism a little bit more?

[0:38:31.4] JP: Yeah, absolutely. When Bitcoin is being mined, currently a block is mined every 10 minutes, which basically means every 10 minutes, all the miners in the network they grab a bunch of transactions, they bundle them up and then the one that produces the most proof of work that has the highest hash rate solves the mathematical problem basically.

The quickest gets the privilege of writing to that block fit 10 minutes. What that means is that there is this just a huge bottleneck in Bitcoin and this block, which is limited currently to 1 megabyte in size, can only be written every 10 minutes and by only one person.

Spectre and phantom basically take that and say, instead of being this synchronous kind of just one block after the other chain, we could instead have a network that uses something called the directed acyclic graph, which actually has multiple branches and nodes that you basically have multiple miners committing blocks at the same time and eventually they're consolidated back into history and it all remains immutable and cryptographically verified.

By doing that, you essentially remove that blockage. Instead of just one megabyte block being mined every 10 minutes, you could have three. Or you could decrease that time to one minute and you could have 10 blocks being written every one minute by multiple miners out there. Yeah, I think it's really an interesting technology.

[0:39:55.9] JM: Okay. Is that like you've got the mem pool of the transactions that have not been confirmed and the different miners, they're assembling blocks from that mem pool. Because of the way that that's done in Bitcoin, there's a lot of duplicated effort. There's a lot of essentially wasted effort. If you were to separate that mem pool into disjoint sets of transactions, then you would not have that wasted effort and you would have higher total throughput.

[0:40:28.2] JP: Exactly, yeah. It basically distributes the load, the network load in a way that doesn't compromise consensus.

[0:40:36.6] JM: You have to admit, that adds a degree of complexity. That's the thing, you got to love Bitcoin's elegance or simplicity there. Then again, maybe I'm just saying that because I'm biased towards seeing Bitcoin function. That's what's funny about this and I think we had a brief conversation at this decentralized Fridays event that you have.

You were talking about your skepticism of proof of stake. I think, if I understood correctly, your skepticism stemmed from the fact that it's unproven, or maybe you could talk about just why you're skeptical of proof of stake. Because I see this is a slightly more complex, unproven consensus mechanism.

[0:41:17.6] JP: Yeah. The problem that all of these consensus mechanisms or trust models are trying to solve is the notion that it has to be costly for somebody to lie, or it has to be costly for somebody to try and attack the network. If so, you have the right incentive structure in place to minimize attacks.

Bitcoin does this by essentially saying the person with the most hashing power in the network wins and they get to mine a block every 10 minutes. Proof of work is a pretty battle tested way of solving this. It's very wasteful and that you have a lot of people competing and doing duplicative work for really only one outcome. Only one person is rewarded and it's very wasteful.

In this other system, so proof of stake, proof of stake essentially tries to eliminate that and instead of having to put down your electricity which costs money, I'm making it expensive to attack the network. You have to bond or stake coins where you say, "Look, I already have a million of these coins in the network and I'm going to essentially put down a security deposit for those. If I lie, I lose them." Again, that's the incentive for the person to not lie.

I think the challenge for that – well, there is a couple of challenges. The challenge with that is coming up with a crypto-economic system that can't be gamed. Like you said – well what I just mentioned, with spectre I think proof of stake to even higher degree has to add a lot of complexity on these rounds of voting and that kind of stuff to basically make sure that that system where all you're staking is –

The beauty of proof of work is that you're staking something. The thing you're putting at stake, or the thing that you're burning money on is a real-world resource; electricity and computing power. When the thing that you're putting at stake in a proof of stake network is just digital money, which doesn't have any tangible representation. It actually doesn't cost you anything, except if that money is worth something to you, right?

There's all these incentive structure you have to have to try and make that work. It also, because that money is digital, there's a problem in proof of stake hold than nothing at stake problem, where there is no incentive for you not to try and gain the system. In Bitcoin, you have to be selective where you point your proof of work, because if you point it in the wrong place, or you try and mine a block – well let's just say you lose everything. You have one shot every 10 minutes.

In proof of stake, I can stake those coins, but then – this is getting a little technical, but I can try and mine multiple chains and forks, because there's no incentive for me not to. I can do that. It's just digital money. I think that's a huge problem that the whole network is going to solve. Then also you just have the same problem that exist in Bitcoin. You have people complain about miner centralization, like global money palace in China, electricity is cheap.

Eventually, you end up with similar problems in proof of stake, where you have these whales who are sitting on a large sum of money. You have the billionaires who again control the network. It doesn't really fix the problem of centralization. It could actually get a lot worse, because rather than having to geographically go and find cheap electricity, if you have money anywhere in the world, you can become a lot of one of the largest validators in proof of stake.

There's some of these protocols trying to solve that by adding algorithms, which try and randomly select a staker, a validator from that pool, but the challenge there is randomness is hard as any software engineer will know. You also guaranteeing that it can be hard as well. There's been some attempts to rein that in and see things like – something called delegated proof of stake, which is how the bit shares and steam, and I think Eos will also function.

These all introduce something called master nodes, which again archived, centralized validated sets. For as wasteful as it is, I think proof of work is probably the most battle tested and proven and has the ability to be the most decentralized, because you physically have to burn electricity to play.

[0:45:28.1] JM: Do you agree with the hypothesis that proof of stake makes sense, because the more of a currency you have, the more interest you have in its succeeding long-term?

[0:45:46.5] JP: Yeah. Obviously, and that's the very basis of proof of stake, right? That's the whole concept is why would I try and tear down something that I'm invested in? Yeah, absolutely. I think, how do you make sure that that person is punished if they do lie and how do you incentivize them against finding different attack vectors, where it looks like they're still – they're not lying, but they actually are, which is what the whole nothing at stake problem is, which basically says if you have enough money, like what's stopping you from going back and changing history and by forking off and creating multiple fake forks?

The way that systems – Bitcoin derivatives and bit committed proof of stake have tried to do this is they implement something called checkpointing, where they have the hashes of history. They basically take the whole chain in a certain blockade and they hash the whole thing. They hardcode those hash checkpoints into the source code, so that even if somebody in proof of stake wants to try and lie, they could only lie back to a certain point.

Again, the systems to try and circumvent and fix this nothing at stake problem. It's just that they all to date have introduced some level of centralization that centralizes this stuff more than Bitcoin inherently, or the theoretical level is.

[0:47:03.2] JM: Let's discuss something totally different, which is Ripple and Stellar and their respective consensus protocols. Ripple is a PBFT consensus system. How does a PBFT system compare to Bitcoin?

[0:47:19.8] JP: Yeah, so PBFT, or Practical Byzantine Fault Tolerance is simply like – if you have a group of say 10 people, how do you make sure that they're lying to one another? It's a

pretty simple round robin process, where you basically have to make sure that 66% of the people all agree and formed consensus.

It's very basic and PBFT has been around for many, many, many years, like longer than Bitcoin has. The PBFT actually works really well and it's used actually in a lot of software platforms. You have technology such as Raft and Paxos, which do orchestration of virtual machines and servers and stuff like that. I'm sure a lot of people that have worked on AWS and things have used these before as a way of maintaining quorum between, say a bunch of Hadoop nodes or service.

The problem with this model is that it really only works in what's called a closed membership setting, which is where you have control of, or you have a predefined set of participants in this equation. You choose the 12 valid data and there is some level of trust in that and say, "Yup, these nodes are not malicious. We know they're not going to lie."

In the case of Ripple, Ripple implements PBFT and they have to approve the valid data in the network. They say, "Hey, banking partner. Can you spin up on this service and run it?" We just trust that you're not going to lie. They're not a 100% trusting that person, because 66% of that trusted valid data is still do need to agree, or the network fails. There's a heavy degree of centralization there.

Stellar is a little bit different and it implements something called Federated Byzantine Agreement, which essentially takes the same model. It's important to note that Jed McCaleb, he founded Ripple, but then he also founded Stellar. They brought in a research scientist, David Mazieres, I think his name is, who wrote the Stellar consensus protocol.

It takes PBFT and it basically federates the membership model to a point where the network itself decides who the validated set is and there' quorum about that as well. I'm actually a huge fan of Stellar. I think that it's a very interesting compromise and solution to this problem.

[0:49:37.1] JM: Although, once again you have the complexity tradeoff. I completely agree with you that we still have not really seen applications build on these things. We haven't really seen peer-to-peer cache be widely used. I'm all for the widespread experimentation.

[0:49:52.1] JP: Yeah. The thing there is I think that Stellar is complex, but I think to the end user it is not. I think that there's a bunch of nodes running for an end user that's using a wallet. Just like Bitcoin, you don't really see the miners. You don't see how that's all working.

That's actually one of my other critiques of proof of stake is that proof of stake greatly – for it to be truly decentralized, it greatly complicates the user experience, because no longer am I just logging into an app that looks like Venmo, but is actually sending around Bitcoin.

I'm logging in and I'm going to be prompted as to whether I want to stake my coins and potentially become a valid data, which I don't think anybody that's using Apple Pay or Venmo right now wants to think about bonding coins. I think from an end-user perspective, I think it's just going to be a lot more complicated for people to understand.

[0:50:42.3] JM: In the last several months as you've seen all these new protocols and new coins come out, how do you decide which ones to actually spend your time analyzing?

[0:50:53.7] JP: Yeah, that's a good question. I try and determine which technologies that new investors taking existing codebases like Bitcoin and simply augmenting them. That tends to help mostly the technologies who just mentioned really different codebases. That's how I judge it, because I think while incremental and proving on Bitcoin is useful, I think more often than not, the coins that a Bitcoin forks really just cash grabs rather than people actually trying to move the space forward.

That's my way of looking at it. Also just keeping a very close eye on the research community around Bitcoin and looking for whitepapers, be in Mimblewimble, or spectre or phantom. I think there's a lot of good work there happening. Again, it's all academic. It hasn't actually been released yet. If you want to node out on it, I think that's the stuff that I gravitate towards, rather than whatever the latest ICO is that's being marketed to me on Instagram and Facebook and everywhere I go.

[0:51:51.4] JM: As we wrap-up, the thing that I think people are waiting to see if the other show is going to drop on is tether, or I guess that's one of the things right now. Basically, tether this

purported stable coin that has not been able to prove that it has a dollar backing each unit of tether cryptocurrency, which – I shouldn't say crypto – tether currency. It's not even really technically a cryptocurrency, right? It's just a currency.

[0:52:19.3] JP: Well, tether is a – it does have a cryptographic protocol, called Omni which operates on top of Bitcoin. It's a crypto-token. You can think of Omni as similar to Ethereum, but build on top of Bitcoin. Yeah, it's like an [inaudible 0:52:31.6] in a way.

[0:52:34.1] JM: Is there like a rational explanation for tethers' resistance to auditing?

[0:52:40.7] JP: No. There's no rational explanation. I think, like if you come with this stuff from [inaudible 0:52:45.5] raiser and where the simplest explanation is often the right one. I think when you're in that industry, in that financial industry and you're not providing audits, it's pretty obviously trying to hide something.

Some of the statements that had come out around, you know them breaking ties with Friedman who was there, or Tony's who were doing the audit previously the statement said that they – things were going too slow and they were being too thorough with the audit. I think if you close ties with your auditor, because they're being too thorough then that obviously speaks volumes as to where things are at.

I don't know. I've commented a lot on tether in the last couple months, but it hasn't gone and self-imploded yet. Maybe it never will right until the game is up. Maybe tether won't fail until the rest of the space sees a huge market correction, but you know. I think there's a lot of red flags, but there's no hard evidence, which is the tricky bit.

[0:53:41.9] JM: Yeah, could be like the herbal life of cryptocurrencies.

[0:53:45.3] JP: That's a really good analogy. Yeah, I think it's hard to get any actual hard evidence on them.

[0:53:51.3] JM: Okay, Jackson it's been great talking to you. I really appreciate you come on the show.

[0:53:54.7] JP: Yeah, thanks Jeff. Thanks for having me on. Really liked it.

[END OF INTERVIEW]

[0:54:01.7] JM: If you are building a product for software engineers, or you are hiring software engineers, Software Engineering Daily is accepting sponsorships for 2018. Send me an e-mail jeff@softwareengineeringdaily.com if you're interested.

With 23,000 people listening Monday through Friday and the content being fairly selective for a technical listener, Software Engineering Daily is a great way to reach top engineers. I know that the listeners of Software Engineering Daily are great engineers, because I talk to them all the time. I hear from CTOs, CEOs, Directors of engineering who listen to the show regularly. I also hear about many newer, hungry software engineers who are looking to level up quickly and prove themselves.

To find out more about sponsoring the show, you can send me an e-mail or tell your marketing director to send me an e-mail jeff@softwareengineeringdaily.com. If you're a listener to the show, thank you so much for supporting it through your audienceship. That is quite enough, but if you're interested in taking your support of the show to the next level, then look at sponsoring the show through your company.

Send me an e-mail at jeff@softwareengineeringdaily.com. Thank you.

[END]