EPISODE 561

[INTRODUCTION]

[0:00:00.3] JM: Laura Shin is the host of Unchained, a podcast about cryptocurrencies and decentralized technology. For every episode, Laura does significant research and preparation so the content turns out polished and high-quality. Her enthusiasm for the subject of cryptocurrencies comes through in her reporting.

Podcasting about cryptocurrencies requires walking a fine line. Cryptocurrencies have a mixture of drama and exciting technology, which are both great for a journalist, but you can't get too deep in the drama because the podcast will feel like a tabloid, and you can't get too deep in the technical weeds, because the listener will fall asleep. There is a fine line to walk.

Laura joins the show to discuss how she got into reporting on cryptocurrencies, why she got so obsessed with the subject and she also discusses her experience as a solo entrepreneurial journalist, which I can relate to.

Before I begin today, I do want to mention Software Daily, which is a place that we have created to post software projects and discuss them with other people, as well as discuss the podcast. You can go to softwaredaily.com and post your software projects, or discuss the podcast. If you're posting a software project you can find collaborators and feedback for your project

It's great if you have an open-source application, or a side project you've been tinkering with, or an academic computer science paper. We would love to see all those things on softwaredaily.com. If your project is especially interesting, we will send you a Software Engineering Daily hoodie, or a t-shirt, or we might even have you on the podcast to discuss what you're building.

I've been posting some of my own side projects and I would love to see what other people in the community are working on. Actually I'm looking at the community right now and there are two recent blockchain visualization projects that are on the forum at the same time which is

interesting. If you want to post your own stuff, come to softwaredaily.com. I'd love to see you there.

With that, let's get on with this episode.

[SPONSOR MESSAGE]

[0:02:22.4] JM: Azure Container Service simplifies the deployment, management and operations of Kubernetes. Eliminate the complicated planning and deployment of fully orchestrated containerized applications with Kubernetes.

You can quickly provision clusters to be up and running in no time, while simplifying your monitoring and cluster management through auto upgrades and a built-in operations console. Avoid being locked-in to any one vendor or resource. You can continue to work with the tools that you already know, so just helm and move applications to any Kubernetes deployment.

Integrate with your choice of container registry, including Azure container registry. Also, quickly and efficiently scale to maximize your resource utilization without having to take your applications offline. Isolate your application from infrastructure failures and transparently scale the underlying infrastructure to meet growing demand, all while increasing the security, reliability and availability of critical business workloads with Azure.

To learn more about Azure Container Service and other Azure services, as well as receive a free e-book by Brendan Burns, go to aka.ms/sedaily. Brendan Burns is the creator of Kubernetes and his e-book is about some of the distributed systems design lessons that he has learned building Kubernetes.

That e-book is available at aka.ms/sedaily.

[INTERVIEW]

[0:03:58.2] JM: Laura Shin, you are the host of Unchained and Unconfirmed, two of my favorite podcast about cryptocurrencies. Thanks for coming to Software Engineering Daily.

[0:04:06.5] LS: Thanks for having me on the show.

[0:04:07.9] JM: You started covering cryptocurrencies in 2013 for Forbes. What was your perception of cryptocurrencies in those days?

[0:04:17.1] LS: Well, actually so just to correct, I actually started in 2015. I think maybe in 2013 I might have written a couple articles, but definitely had nowhere near the understanding that I later obtained when I began covering it more regularly. While some early articles did come out at that time, I definitely would not say that I started covering it then.

However when I did start paying more attention in 2015, those were the blockchain, not Bitcoin years, which was back when a lot of Wall Streeters got interested in the technology, but because at that time Bitcoin was affiliated with the dark web and often thought of it as criminal money, I think a lot of them shied away from showing an interest in Bitcoin itself.

Frankly, if we think about it because bitcoin is a peer-to-peer payment system and many of these other crypto-assets are peer-to-peer payment systems, they basically cut out middlemen, like financial services institutions. I think a lot of them, thought that they could use blockchains to make their services more efficient, and thereby preventing the disruption that could happen from a service like Bitcoin that is peer-to-peer and cuts out the middlemen.

At that time, I actually thought that there was something to that frankly, which I'm a little bit embarrassed to say right now, because as we've seen I think we can all say that the public blockchains are so much more powerful and interesting than anything going on in the private sector.

However at that time, I remember that I interviewed Coinbase. At that time, I was a freelancer for Forbes, but they had put me in charge of what they – new list they were launching called the Forbes FinTech 50 list along with another reporter at Forbes, and she and I divvied up the list into different categories and each took a category and I took digital currencies.

I remember that when I vetted Coinbase for the list, I was trying to get them to explain how Bitcoin would be adopted, because this was the days when Bitcoin had crashed down from a high of more than 1,200 down to – it was languishing in the $200 range. They said, "Oh, well it's a lot cheaper than Visa, and so you save on the fees." I said, "Oh, but consumers don't pay the fees, so how are they going to know that they're saving anything?" They said, "Oh, well the merchants can pass on a savings of 1% and he's sort of the – I think with Bitcoin."

I remember thinking this is totally not convincing and I did not put them on the FinTech 50 list. Instead I put these more enterprise blockchain companies on the list. It's just so fascinating to fast forward a few years and everything has changed, and it's so different now. That was really my impression at the beginning. I really thought, "Oh, wow. This is going to make our financial services more efficient and it's going to enable these companies to offer new products and services that were not possible before with the existing financial infrastructure."

[0:07:40.5] JM: What you're referring to there about being mildly embarrassed about making some early incorrect judgement calls, whether it's not calling private blockchains, by the way to the point private blockchains is still very early, private blockchains could be very impactful, they could be very important. We still don't quite know yet, but I think all of us, I mean most of us made some error in judgment early on when they were watching this space from afar.

I feel like one nice lesson of watching cryptocurrencies rise and even as I was covering it and not really taking part in it as an investor, or really taking it seriously other than just covering it at a skin-deep level, it's just made me realize that I'm not very open-minded and that I need to be more open-minded when it comes to technology and new ideas, because I didn't take it seriously for the first eight years and it makes me question my own open-mindedness.

[0:08:42.6] LS: That's interesting. There's a couple things I want to say to that. First, I disagree with you about how it's too soon to tell whether or not private blockchains will be transformative or not, because I think we know enough to say that first of all, these companies move too slowly, I think, to really do anything that will keep pace with the disruption that we're seeing over on the public blockchains, first of all.

Second, I think just the idea that using a new technology to upgrade your systems and make them more efficient that that would be revolutionary. I don't see that at all. If we look at some of the really big trends that have been happening in the public blockchains like that is all super, super new.

It is as we've seen with the regulators, this is like just creating a whole new category of assets and that function in ways that previous assets just never functioned before. I think just if we look at how global in 24/7 and fast these are, there is just really no parallel in the existing financial markets.

I've been frankly don't have a huge background in financial services, but from what I can tell the only thing maybe that comes close to these markets just even on a pure fact of them being open 24/7 365 is foreign exchange or something, which apparently the last market for that closes Friday night. What is that? Like Australia time or something, and then 36 hours later roughly the next market opens I think, somewhere in Australia. I forget. Someone explained this to me, but I might be mixing up the geographies. The point is, even that's not 24/7 365.

That was the first thing I wanted to say. Then the second part is that actually, so I was a little bit different from you and that I – once I truly understood the technology, which like I said, that only really occurred in 2015. I don't know if I could see exactly where it was all going, but I definitely knew this was perhaps the biggest thing I'd ever learned about in my entire career. I knew right away that I only wanted to write right about this.

Well actually, that it took me a couple months. I definitely knew that I was obsessed in a way I've never been obsessed with anything before ever, other than things in my personal life yoga, or Argentine tango, or – I remembered that I took this trip and I had this other book idea that I was working on, and it was a working vacation. It was this writing retreat that I had set up for myself.

I remember that I couldn't get the work done on the original idea, because I kept looking up and reading about Bitcoin. Definitely from the start, there was something about this that just really grabbed ahold of me and made me feel like, "Whoa, this is going to be huge and this is going to change everything over the next few decades," and I still think that.

[0:11:55.0] JM: 2015 that means you were getting into this around the time that Ethereum launched. Were you skeptical of Ethereum, or did you take that one seriously too? Because that was one where I had been talking to some Bitcoin maximalists when Ethereum came out, and I was convinced by them to be very skeptical of this thing that I've now become – I've totally reversed my standing on and that was another incident where I was like, "Oh, I really should not let myself be overly swayed by the strong opinions of anybody in the space, and I should really just take everything with a grain of salt," because once again I was overly skeptical of something. Of course, you do need significant skepticism in the area, but when did you get convinced of Ethereum? Were you an early understander, or were you skeptical from the early days?

[0:12:45.1] LS: I did not even hear about Ethereum when it launched, because when it launched was about two months after I even learned what a blockchain was. I wasn't quite into it enough, but also I have to say I was working on this huge magazine story. It literally ended up being the longest magazine story Forbes Magazine ever published, now is about blockchain technology and financial services.

I was a super, super deep in this other world and did not care about Ethereum until a while later, but I remember that I did not have the experience you had where a lot of Bitcoin maximalist treat it – taught me to be a skeptical of it.

Instead, I had a lot of sources saying that this was the next big thing and that they thought a whole bunch of developers were moving over to that, that had a lot more potential, because of how limited the scripting language was in Bitcoin. It's funny, because I'm not a technical person, so it took me a while to understand what they meant by that.

Now obviously, I mean we've seen such huge trends come out of Ethereum. It's like the DAO, the initial coin offering trend, cryptokitties. Nnow I fully understand, "Oh, this is –" it's not even now, but earlier like a year or two, actually it was more summer 2016 where I think I really started to grasp the full potential of Ethereum, because that was when everyone started telling me about what they were calling app coins at the time, which is so funny.

It's so funny how – yeah, even back then we didn't have the term crypto-assets, I think. I remember that I wrote about a white paper that Chris Burniske who's one of the premier analysts in the space, co-wrote with Adam White of Coinbase. I remember that the white paper list about how Bitcoin heralded a new asset class, but they didn't have a name for it.

I remember that they were batting about different names in the white paper, like literally saying we could call it these different things. I don't remember all of the names, but one of them Chris and I actually we're just laughing about recently was Consensobit. I think crypto-assets is much better, but – Yeah, at that time people just really – they knew something new was happening and they understood, "Okay, this is a new asset class, these are investible," and they can have all different applications and different functions. For that reason, you will use them in different ways. Yeah, it was just so new I remember Brian and Fred where they called it Wall Street 2.0.

Oh, my God. It's so funny to look back at these conversations I was having back then, because now the space moves so fast that even just in I guess like a year and nine months everything is quite different.

[0:15:44.7] JM: It already has that dated dusty flavor when you look back at magazine articles from 1994, 1997 when they're talking about the internet.

[0:15:55.0] LS: Right, right. We do that at warp speed, because now we have the internet to facilitate our conversations about all this stuff.

[0:16:02.3] JM: Yeah, the parlance updates much faster.

[SPONSOR MESSAGE]

[0:16:15.3] JM: Users have come to expect real-time. They crave alerts that their payment is received. They crave little cars zooming around on the map. They crave locking their doors at home when they're not at home. There is no need to reinvent the wheel when it comes to making your app real-time.

PubNub makes it simple, enabling you to build immersive and interactive experiences on the web, on mobile phones, embedded into hardware and any other device connected to the internet. With powerful APIs and a robust global infrastructure, you can stream geo-location data. You can send chat messages, you can turn on sprinklers, or you can rock your baby's crib when they start crying. PubNub literally powers IoT cribs. 70 SDKs for web, mobile, IoT and more means that you can start streaming data in real-time without a ton of compatibility headaches. No need to build your own SDKs from scratch.

Lastly, PubNub includes a ton of other real-time features beyond real-time messaging, like presence for online or offline detection and access manager to thwart trolls and hackers. Go to pubnub.com/sedaily to get started. They offer a generous Sandbox to you that's free forever until your app takes off that is. Pubnub.com/sedaily, that's P-U-B-N-U-B.com/sedaily.

Thank you PubNub for being a sponsor of Software Engineering Daily.

[INTERVIEW CONTINUED]

[0:17:58.5] JM: At this point, I am pretty excited about Ethereum too. Although compared to what people are really excited about, which is that you can have this decentralized world computer, there's not a whole lot of applications that have actually been created on a theorem. You have lots of dApp coins, but not a whole lot of dApps. Really the only applications we've seen from Ethereum are the ability to make a token, and the ability to make scarce collectible items via the cryptokitties sort of thing.

I guess, you could also say smart contracts, maybe there's some usage of escrow style things, although you could do that on Bitcoin. Do you have a sense for when these dApps are going to actually happen on Ethereum, or what the bottlenecks are?

[0:18:53.1] LS: Oh, gosh. I mean, this is what is so interesting about the ICO craze and comparisons to '99 and 2000. I think as we saw in '99-2000, a lot of how this stuff matures depends on infrastructure. Even as we had back in the early days of the internet, people saying things like, "Oh, people are going to buy their groceries on the internet, so Webvan is a good idea."

It actually was a good idea. It's just that the timing wasn't right. Now we have Instacart. I use Instacart. I'm sure I know that now Amazon owns Whole Foods. They started a service where you can get your groceries in two hours. These are things that really did happen and got built, but the timing wasn't right.

I don't think it's quite fair to criticize Ethereum just yet, because there are so many basic functions of crypto-assets that have not been built out that need to be built out. I mean, just though the most basic, which I know a lot of people are working on this year, I can think of just five different companies on the top of my head that are working on this at different levels for different types of customers, but Custody is one of them, right?

I've written about this before, but it is so easy for individuals to have their Bitcoins or other crypto-assets hacked. This is different from saying that a blockchain can be hacked. I know that a lot of people have this misconception that because some exchanges have been hacked, or that because individuals have lost their tokens, that means that these blockchains are insecure. That's not the case. It's just that they function differently from the traditional financial services system, where a company will manage your assets for you, right?

Even then, I was just talking with Ari Paul on my podcast and he made the good point that financial services hasn't really solved the problem either. What they have done is they've just put tons of insurance in physical bodyguards and physical – and gates around these things. I actually found that a really fascinating point.

The thing is that dealing with crypto-assets requires a fundamental psychological shift in the way you think about money and in the way you handle money, because it truly is digital cash. When we think of things that are digital, generally we think, "Oh, my bank interface on the web, that's me like – or PayPal or Venmo. Oh, that's me moving money digitally."

No it is not, because it's what's happening on the background is that all these banks have their own ledgers and then they all have to meet up afterward and be like, "Okay, did we get it right? Is that how much – if you subtract that amount from person A who's sending this amount to person B, then I have to add that same amount to person B." They have to make sure

everything's reconciled, right? Essentially on the back end, it's not that different from what people were doing 600 years ago with double-entry accounting.

Here, you have something that's truly digital, like literally a digital asset. You can lose it like a dollar bill from your pocket. You lose the private keys essentially. You can and actually even lose those private keys just by somebody seeing the private key, right? It's not even about literally dropping it, like I said about the cash. It's just, oh if you expose this, if it becomes visible to somebody else, then they can send them the money out of your wallet.

We are literally at the phase where we don't even have the basic infrastructure to make the dApps usable by a lot of people. If you followed any of the scaling debates in Bitcoin and Ethereum and just – or not even debates, but the fact that a lot of new blockchains are trying to tackle the scaling issue, then you will obviously know that blockchains themselves right now cannot support a lot of users.

I feel like the way that I often think about is back in the early days of the internet. AOL started with, what was it? Like 14.4 kilobytes per second in dial-up connection. Then it became 33 or something, and then it went to 56. I remember when it got to 56, I was excited. Basically, that's where we are with blockchain. Not even at 56, just to be clear. We're definitely at a phase below that, I would say.

That's why a lot of people are talking about some of these scaling solutions that are either happening right now, or are being talked about right now, because they know that that is a big problem that needs to be solved for. I would personally say at the moment that custody and scaling, or some of the main ones that I think about. That's why when I get these pitches for ICOs, anything that's a little bit more consumer-facing I'm a lot more skeptical of, just because I don't think the technology is at a point yet where we can really onboard a lot of users and have them using the blockchain in any really high transaction volume fashion.

[0:24:15.0] JM: Yeah. Speaking of scalability there, the one scalability story that I have not been able to cover as much as I would like is that of Lightning Network. Lightning Network is a divisive topic. Do you think that Lighting Network is going to solve scalability for Bitcoin as a payment solution?

[0:24:35.9] LS: I'm not sure. I haven't done a really deep dive into Lightning Network, I have to say. The main things that I do know about it are that some of the concerns are that it centralizes services, like some of these lightning companies – it's not like Bitcoin which is this peer-to-peer software, but you end up using a company for that I think.

I know that that is one of the concerns and I know that that is why some of the people that wanted to increase transaction throughput on the Bitcoin blockchain were advocating, for doing it directly through Bitcoin itself. The reason on the other side that people were cautious about doing that is that if you wanted to do that, then you would need to do what's called a hard fork in Bitcoin, which had – which ran the risk of splitting the chain

Of course, because the two sides on both sides of this debate got so entrenched, we didn't end up with a fork and that's how we have Bitcoin cash. .Really now we essentially do have these competing visions of Bitcoin in the marketplace. We'll see which one is able to scale better.

Another thing that confuses me about lightning a little bit, and I have not – like I said, I haven't done a deep dive, but as far as I understand in order to open a lightning channel, you need to put up a little bit of money. Let's say you and I are transacting in some fashion and I think maybe the amount that I'll end up paying you is somewhere between like, I don't know a 100 and 500.

Well, since I think the upper bound is 500, I should put the 500 in. Then that ties up the money while we trade back and forth. I just wonder, how many people are going to want to tie up their money in that way before they close the channel and cash out? That's another question that I have about lightning.

It's such early days that there's really no way to make a good judgment right now. I know that essentially a lot of people don't think it's possible to put a ton of transactions on the Bitcoin blockchain, nor is it necessary. Because of things like environmental considerations and just wanting enough people to be able to run what's called a full node, which is where you basically download the entire blockchain, which is the ledger of all transactions going back to the first transactions in January 2009, they want people to be able to do that.

In order to make that happen, it's better to keep the blockchain as light as possible, so that it enables more everyday people to do such a thing. For that reason, they feel like lightning has a lot of potential to help ease that bloat basically on the Bitcoin blockchain.

[0:27:29.9] JM: Right. To the $500 locked-up point, I think it will be locking up $500 in a Venmo account. I use Venmo frequently enough that if I have $500 sitting in Venmo, I don't immediately cash it out, I don't really care because I figure I'll just be transacting with it enough in the future. In any case, that payment channel will have some expiration date eventually whenever the contract, the hash time lock contract expires.

[0:27:59.4] LS: Yeah, but the difference is that with Venmo you can interact with a lot of different people, but with Lightning Network aren't you just interacting with the person that you open the channel with?

[0:28:08.8] JM: No. The idea is that you open the hash time lock contract with one other person is the base case example. The idea is that you would – I think you can have multi-party contracts where I could open up a contract with you and three other people and maybe it's a little more elaborate, and then you can also have other contracts that are off chain that are opened between you and let's say Sharon. That way, I can transact between myself and Sharon by shuttling money through you off chain.

I think one of the big concerns around this is well, okay then that leads to lots of off chain transactions and some people believe that that is recreating the banking system. To some degree, the banking system needs to be recreated, which is what I think you were somewhat alluding to with your discussion with Ari Paul there, like, okay –

The traditional banking infrastructure, we've got security systems and guards and vaults and stuff. If we're the crypto anarchists, maybe we're critical of those things, but if we're the average citizen, we want those things. I think what's nice about Bitcoin is you have the option if you want to transact everything on chain. I don't think there's anybody who has a roadmap that eliminates the ability for you to do that. What we're talking about here is the building out of infrastructure to make things more accessible to other people.

[0:29:35.7] LS: Yeah. I mean, what I would say is I think that people on the big block side say that when we get a lot of adoption, then the fees will go too high, if that is the one – the option that you want to pursue, which obviously we did see at the end of 2017, where fees were like – the average fee was 60 some dollars.

Going back to your point about how the Lightning Network was similar to the banking system, that's what I meant earlier also about how it does centralize a little bit. I do think that it's really about what trade-offs you want to make. That's why we ended up with these two camps. There's one camp that's more willing to make certain trade-offs and not others and the other camp it goes in the other direction.

That's why I feel like some people with the lightning side, they maybe don't care as much that the users get centralized onto these Lightning Network services, but they like the fact that then that also enables people who might want to run a full node to run a full node on Bitcoin. Then on the other side, you have people who say, "No, we want everyday consumers to be able to transact on the Bitcoin network itself and not have to use a company at the lightning level and also therefore, when they use Bitcoin not pay high fees."

Then the ability to run a full node is impaired. I think it really just – it just boils down to, like there's probably some spectrum and then half the – not even half, but some portion of people fell on one side and then another portion fell on the other. It's one of those things where, yeah – like I said, I do not consider myself an expert on lightning. I haven't done enough interviews on that topic at all to really have a strong opinion one way or the other. I definitely know that here we have two coins in the while that are directly competing on this very issue, and so we'll see which one prevails.

[0:31:36.9] JM: Okay. I mean, that makes two of us in terms of the lack of Lightning Network expertise. Okay, so you're talking there Bitcoin cash, the thesis there is that all of the transactions are going to take place on chain?

[0:31:48.8] LS: Yeah. I think that's what they think at least for now, that's why they have this 8 megabyte block.

[0:31:57.0] JM: Okay. Yeah, that's another topic I didn't fully comprehend. I did some shows on the segwit fork. Can you just give me an abbreviated story about what happened there? I know you just touched on it lightly, but maybe just fill us in on what were the events that led to the Bitcoin cash instantiation?

[0:32:20.1] LS: Yeah, I mean it goes back to this debate that I just described about how some people think that it's more important to keep Bitcoin decentralized in such a fashion, where individuals can run full nodes. I think the other thing that they want to keep decentralized there is mining, which has become quite centralized on Bitcoin.

At some point in the past actually, there was one mining pole that even approached 50%, which in Bitcoin is a dangerous thing, because then the network is susceptible to what's called a 51% attack. Where some actor can gain control of more than half of the nodes in the network and therefore, they can pull shenanigans with the blockchain basically by excluding certain people's transactions putting in their own, changing past transactions, etc.

I mean, it is a little bit limited, like you can't do a ton, like you just for the amount of hash power required, you basically could reorg transactions in the most recent blocks. Still it's something that the community is very cautious about. Because we already do now have these mining pools where they have 20%, 25%, maybe even 30%, the proportions change a lot.

There is concern about mining centralization. That was another reason why people wanted to keep the block – what's called the block size in Bitcoin, which is it's like a limit to the amount of transactions that can go through at any given moment. That was their reasoning for wanting to keep it at that.

On the other side, you had people saying, "Hey, Satoshi didn't even want to put a limit in. He was just persuaded to put one in, simply because I think it was Hal Finney was who was this other person. Gosh, I don't even know if he was a cryptographer, or what his role was, but he is somebody who had previously also worked on some of the precursors to Bitcoin and got involved with Bitcoin very early. In fact, I think he was the first person that Satoshi reached out to. No sorry, Hal was the first person who responded to Satoshi after Satoshi published the coin white paper.

Anyway, the point is that Hal, I guess persuaded Satoshi to put this limit in, because he said, "Oh, I don't want people to spam the network and overrun it." The people on the big block side say, "Hey, this was never even meant to be here in the first place." Now that we have a lot more adoption, a lot more people are using the blockchain.

The fees are going up and it's making Bitcoin unusable for certain groups of people that transact in small amounts and particularly – those tend to be that people who don't have access to the really good financial services that we have here in the US. There are people in developing countries who can probably benefit from Bitcoin more than and anyone else.

Those people would say that running your own full node isn't that important and that the – just gaining adoption and increasing the limit at a pace that can accommodate all the new growth that might occur, that that's more important, because we're out of phase right now where it's so early, that the more important thing is just to get a lot of adoption.

Like I said, I think some of those people also have concerns that if we try to move people to what's called layer 2, which is what you were asking about earlier, the Lightning Network, then they worry that then it centralizes Bitcoin in a different way, which is having users interact with companies rather than just peer-to-peer on Bitcoin.

These arguments literally I went back and forth for two and a half, three years. It just was getting intense. It was interesting and alarming as I was reporting on this, because I just – I got interested in what was going on and then I just kept following all the different twists and turns and the debate. As time went on, certain people who started off being very diplomatic about the differences and treated this as an intellectual exercise, after a while they would say things like, "I refuse to work with so-and-so." It just got very personal and nasty.

That was how we ended up with this group that wanted to basically split off. They finally did and they created Bitcoin cash. They have a road map that – The other interesting thing that they did was the current implementation of Bitcoin has a feature called segwit, or a segregated witness, which is basically a different way of treating what's known as the signatures in Bitcoin. I'm not a technical person, so I probably can't describe that too well, but it's a way of separating out the

data, so that way it doesn't contribute to the weight of the Bitcoin blockchain, which as I mentioned earlier, affects whether or not you can run a full node.

Bitcoin cash also did not adopt segwit. They're actually quite different now. It's not only the block size, but also this feature called segregated witness. Yeah, they're both in the marketplace and competing right now. Obviously Bitcoin has the brand name recognition.

One last thing I would add, which is just funny to watch this instead. A lot of people say that Bitcoin cash is following the vision in the original Bitcoin white paper, which I think actually a lot of Bitcoin people even agree with this now, because essentially the way that the developers of Bitcoin have developed Bitcoin, it's to be more in favor of the digital gold aspects of Bitcoin.

The way that the Bitcoin cash people have developed their version of Bitcoin is to be more in the peer-to-peer payment system vision of Bitcoin, which the Bitcoin white paper's subtitle is a peer-to-peer payment system, or something like that. The last bit that I wanted to say was, so I will grant them that that it is probably true that they are fulfilling this vision of the white paper a little bit more closely.

Then the funny thing is that one of the guys who's the biggest proponent – one of the biggest proponents behind Bitcoin cash is this guy Roger Ver, who in the early days of Bitcoin was known as Bitcoin Jesus, because he was a millionaire when he got into Bitcoin already, and so he had a lot of money at that time to even buy up a ton. He would just give them out to people that try to proselytize people about Bitcoin.

The point is, so he owns the domain name bitcoin.com. Now this website is talking about how Bitcoin cash is actually the real Bitcoin, because it's pursuing the original vision. There's been a lot of tussles, some people view it as propaganda and they're really upset that he's doing this. The whole thing is just – it's just really funny to watch.

Frankly, I actually think that if so, I didn't even answer your question, because okay, just to try to wrap this up, segwit 2X was this point where the more entrepreneurs who were concerned about making sure that the block size remained big enough to accommodate new users, they all got together and they said, "Oh, we want to increase the block size to 2X, but we'll give the

people who want segwit in layer 2, like Lightning Network will give them segwit 2, too but we'll do both.

They were trying to compromise with the two sides and bring elements of what the Bitcoin people wanted and elements of what the Bitcoin cash side wanted into one chain. Ultimately, they ended up if this is the chain that ended up being what we call Bitcoin today, that they adopted segwit first. The segwit part of the deal went through. Then the 2X part did not go through. They sort of chickened out basically to do that, because of the fact that required a hard fork.

Even though that all happened in November and it got decided then that they weren't going to do this fork and increase the block size limit, you still see people arguing about this point all these months later, on Twitter and everywhere. If you look at the Bitcoin sub-Reddit, the BTC sub-Reddit, they still are arguing about this. It's ridiculous and funny to watch.

[SPONSOR MESSAGE]

[0:40:49.3] JM: We are running an experiment to find out if Software Engineering Daily listeners are above average engineers. At triplebyte.com/sedaily you can take a quiz to help us gather data. I took the quiz and it covered a wide range of topics, general programming ability, a little security, a little system design. It was a nice short test to measure how my practical engineering skills have changed since I started this podcast.

I will admit that, though I've gotten better at talking about software engineering, I have definitely gotten worse at actually writing code and doing software engineering myself. If you want to check out that quiz yourself, you can help us gather data and take that quiz at triplybyte.com/sedaily.

We have been running this experiment for a few weeks and I'm happy to report that Software Engineering Daily listeners are absolutely crushing it so far. Triplebyte has told me that everyone who has taken the test on average is three times more likely to be in their bracket of quiz scores.

If you're looking for a job, Triplebyte is a great place to start your search, fast-tracks you at hundreds of top tech companies. Triplebyte takes engineers seriously and does not waste their time, which is what I try to do with Software Engineering Daily myself. I recommend checking out at triplebyte.com/sedaily. That's T-R-I-P-L-E-B-Y-T-E.com/sedaily. Triplebyte, byte as in 8-bytes.

Thank you Triplebyte for being a sponsor of Software Engineering Daily. We appreciate it.

[INTERVIEW CONTINUED]

[0:42:47.7] JM: The issue of the centralization, the fact that Bitcoin is physically centralized, like if a government wanted to wipe out all of the miners, they would know where to go. This is one of the issues with Bitcoin right now is that it's not actually decentralized, at least in the physical sense. What do you think would happen if those miners got wiped out, if China decided no more Bitcoin mining?

[0:43:18.4] LS: I don't agree with the premise of the question, because they're not all located in one jurisdiction. It would actually be quite difficult for all miners to be wiped out. Yes, the majority of them I think are in China, but already we've seen that Bitmain is reading the tea leaves and Bitmain is the biggest – they're both a mining equipment manufacturer and they run some of the biggest mining pools. They're based in China, but already we've seen that they are looking maybe to locate to Switzerland and maybe doing some business here in the US.

I know that Bitfury, granted they're small now, but they have recently done a whole bunch of deals and they run mines, or mining pools in – or not mining pools, but yeah, mines in Georgia, Norway, Canada Iceland. Already, just with the few that I've mentioned, and there's a ton of mining also happening in places like New York and Washington, and I think – shoot, there was one other state I read about somewhere in the West state. I don't remember which one it was, but the point is that I don't think it's possible for any one government to shut down all the miners.

I don't think it's possible for I think the likelihood that all the governments come together and agree to shut down all the miners at once is basically zero, because I mean, we have countries

right now that are opening their arms to these miners, so I definitely – I just don't see that happening.

[0:44:57.9] JM: Are the concerns around the centralization more around the fact that it's regardless how they're geographically distributed, these miners are in the same mining pools?

[0:45:08.1] LS: Each mining pool company – so a mining pool is where – let's say that you and I, just individuals want to mine a little bit of Bitcoin, but we don't want to buy a miner, because it makes our home hot and maybe with the way that the payout would occur if we owned our own little mining equipment was that maybe we would find a block right away, but then not see another one for six months, then maybe then I would get two in a row.

When you join a mining pool, it enables you to even out the cash flow from what you've invested, right? Let's say there's a mining pool that has 25% of the Bitcoin hash power. Then over time, the average amount of block rewards that it will obtain is 25% of all the block rewards being given out. If you and I each own 1% of that mining pool, then we would get that 1% paid out to us in an even fashion. That's the motivation to join what's called a pool.

These companies, when they run pools they often – it's not all their power. That company Bitfury that I just mentioned, they actually are an exception where they don't run a pool and whatever Bitcoins they mine, they keep. Many of these other ones, they run pools where individuals are contributing, but those individuals could choose to go to a different pool if they felt like it.

The power that the miners have could be limited in that regard, because people could vote with their feet. I know that before the segwit 2X debate, there was concern about whether or not the pools would force people to mine on – because there was a question, okay if it splits, will the miners mine on the 2X fork or on the original fork, which had the 1 megabyte blocks?

There was a question, "Oh if you're part of a pool, will they force you to mine on one chain or another?" The thing is like I said, you can switch pools. In that regard, they don't have as much control as you might think.

[0:47:16.2] JM: They do get to choose – the pool as a whole will choose which transactions from the mem pool they're going to work on, right? They all agree, we're going to hit up these transactions and this is going to be our block. They have some censorship potential from the centralization of hash power in those –

[0:47:38.3] LS: Exactly. Yeah. That goes back to what I was saying before about the 51% attack, without as I think what people are concerned about is if any one particular miner were to obtain that level of power, then yeah, they could do whatever they like to probably increase their Bitcoins, or to punish other people in the network.

[0:48:00.4] JM: Okay, there's a bunch of other stuff I wanted to get to. We're definitely not going to get to everything that I wanted to discuss with you, but just to shift topics dramatically, because you're getting of a lot of exposure to the different players in this space and there are so many curious personalities in the cryptocurrency space. That's one of the things that makes it really appealing as a journalist is the people are so variable and strange and powerful and brilliant. It's really a wide range of personalities. It's really fun to cover.

One area of business that is expanding is that of the crypto hedge fund. All of these crypto hedge funds got created during this massive bull run-up. The thing that I don't quite understand about a crypto hedge fund is in 2018, what is your hedging instrument? Because it seems like most of the crypto assets move in a correlated fashion and there's no derivatives market that's developed, I don't think. Do you have a sense for what strategy a crypto hedge fund is taking? Is it more like a crypto index fund?

[0:49:14.7] LS: They all have different strategies. I know that some of the probably more, I guess, prestigious hedge funds are not really actively trading as much. They take a bit more of a venture approach. There are some that do actively trade, but as far as I understand I think they actually keep quite a large amount in cash, or in Bitcoin and ether itself, because of the difficulties of keeping – and the risks of keeping a large amount of coins on exchanges.

I don't have a great insight into whether or not they have fancier tricks for managing big downturns like this. I will say though that definitely – I wrote this article last summer about all these new crypto hedge funds that were opening. The beginning of it was both sophisticated

and unsophisticated investors are getting in this phase. Then I said, "I guess, we'll see which ones survive a downturn." Already a week or two ago, I saw a headline saying like already nine have closed.

Definitely, there are some people who don't know what they're doing who tried to get in and realize, "Oh, this isn't working." Overall, yeah, I think you're right that there aren't at the moment especially really good sophisticated strategies that you can use. Actually there was one, shoot, that – I'm not going to remember this, but there might be a few out there, but I think you're right that especially at the moment, and with the space just as immature as it is, that a lot of them are just doing things.

Like maybe they buy in at the ICO at a discount, because maybe they're funding the project really early or something like that, and then they make money that way, or they keep money in cash, because of the exchange risk. Or they're just long-term holders and they're going to see how their investment plays out over the long-term.

[0:51:20.5] JM: Yeah, well I'm excited to see what will happen when the derivatives market develops. It makes me wonder, is that what's holding back major financial institutions from getting into this space seriously? Do you have an understanding of how the – in mid- 2018, what the JP Morgan's and the Goldman Sachs's of the world, how they're approaching the space?

[0:51:46.4] LS: Yeah. A lot of traditional financial institutions are hesitating, because the markets are small, there's not good custody solutions. Just if you want, especially recently we saw that one of the startups in the space that has focused for years on security called BitGo, they recently acquired what's known as a qualified custodian, which is a type of company that I guess complies with certain rules around custody and assets for financial instruments like ETFs and other kinds of financial instruments. There hasn't been a qualified custodian in the space that will custody additional assets, until I think the acquisition occurred.

Just right now, there's so few options for managing your risk if you are a digital player and want to invest in this space, or complying with whatever regulations. Because we are seeing a number of these custody solutions come online just this year, like Coinbase announced one called Coinbase custody, but that's only for hedge funds and I think the minimum is something like 10 million dollars.

Then there's another one ledger enterprise. There's another one coming out called Anchor, I think, another one that Ari mentioned on my show, Cambrian. Literally people are right now building these things that will probably make financial institutions more comfortable with investing in the space. I think so far for that reason has just been maybe some family offices that have been dipping their toes in. I imagine once the infrastructure gets built out, then we will see some bigger institutional players get in.

[0:53:39.1] JM: I know your time is short. I wanted to ask a little bit about your movement into podcasting, your hard right as a journalist into podcasting. By the way, I think it's admirable you struck out on your own with Unchained and Unconfirmed. You're building your own media enterprise, which I'm a big fan of it.

It reminds me of a conversation I had with Brad Stone last year, so he's a journalist at Bloomberg and he's a phenomenal journalist. He wrote the everything store, he's written a lot of great pieces about Uber. When I interviewed him I asked him, "Why don't you just start your own media company? Why not take out the middleman?"

Because I would certainly subscribe to the Brad Stone channel, but I think, he gave very good reasons, the fact that with Bloomberg, you get all of these benefits. You have people around you who can support you, you have infrastructure to support you, you have a steady paycheck so you don't have to go out pounding the pavement for advertisers, which is what I do. I'm sure it's probably what you do. Why did you start your own media outlet and what's your – given your past experience with Forbes and other places, what's the pros and cons of striking out on your own?

[0:55:00.8] LS: This is an interesting question, because I for most of my life, most of my professional career I've really liked working on my own. In fact, I tend – when I get a full-time job to not stay very long, which makes my mom really annoyed at me. I started Unchained back when I was a freelancer at Forbes. That was during the summer of 2016 when the space was just nowhere near as big or as interesting to the outside world frankly as it is today.

It just grew beyond my wildest imagination, really. Even though I did end up going full-time with Forbes last summer, at a certain point I just suddenly realized, "Oh, my gosh it makes more financial sense for me to quit and do the podcast, which does not take five days of work a week, than it does to stay in this job working five days a week, or even more," because I was frankly totally overwhelmed there. Just plain numbers-wise, it was a no-brainer frankly.

However, that said, like I said before, I had spent a huge portion of my career working as a freelancer. I just really work best for myself. I don't know exactly why that is. Some people they say like, "Oh, I have issues with authority." That's not it for me, but definitely I think if I have some vision for how to execute something, I do much better as a worker than if I'm being told to execute somebody else's vision, like I just don't have the same motivation and drive. Maybe that's part of it.

Yeah, I mean, I grew up in a household where literally my parents, there was not a single rule ever. I grew up with parents who – my sister and I didn't even have a curfew. Maybe I'm just too used to not having people tell me what to do, or something, like I don't know. It has not been a question for me frankly when I've – whenever I faced this choice of being full-time or being on my own. Generally, I've wanted to be on my own.

When I did go full-time last summer, I did think, "Oh, I'm going to be able to execute my vision for how to cover this piece here at this institution." Unfortunately, didn't work out that way exactly. Then once I realized that this other road I could go was not only going to allow me to do that, but also be more – that made more financial sense, then I just immediately was like, "Okay, I have to do this." I had to do it fast, because the crypto spaces moving incredibly fast. I have to say it's worked out quite well.

[0:57:50.1] JM: It doesn't surprise me at all. You're making a great product. I think many of the reasons for having a overseer as a journalist in the past had to do more with distribution and podcast. We saw this start with blogging. Podcasting is even less of a walled garden than blogging, because you're not gated really by Google. In fact, the search experience is just awful, which can work well and – a or search and discovery, I should say, can work well and it can work against. If you're a rogue journalist, I think generally podcasting is a great place to explore, because it's so undeveloped.

[0:58:27.4] LS: Yes. Interestingly, something that I didn't expect out of this whole thing is that last year, people started coming up to me saying, "I love your podcast." Which was so weird, because at that point I'd only done 25 or 30 podcasts and I'd written probably a thousand articles. It was so bizarre, but I think it's such an intimate medium that people really began to associate me with that.

Now obviously I have found a good niche that people are interested in and then they – it's something where the work that I put in somehow, that the benefits have that accrue to me more than if I'd written an article, if you know what I mean.

[0:59:05.8] JM: For sure.

[0:59:07.2] LS: Now it's great, because like I said, I don't spend five days a week working on the podcast, so I have time to do some other projects that I'm working at, which I don't want to talk about too much.

[0:59:16.3] JM: All right, well I hope to have you on again in the future, as soon as you want to talk more about your other projects. I had about 55 other questions that I wanted to discuss with you. For the meantime, I'll just stay tuned to Unchained and Unconfirmed and hope that my questions get answered there.

Thank you, Laura. I love your podcast and I'll talk to you soon.

[0:59:34.6] LS: Well, it's been super fun. Thanks for having me.

[END OF INTERVIEW]

[0:59:40.0] JM: GoCD is a continuous delivery tool created by ThoughtWorks. It's open source and free to use and GoCD has all the features you need for continuous delivery. Model your deployment pipelines without installing any plugins. Use the value stream map to visualize your end-to-end workflow. If you use Kubernetes, GoCD is a natural fit to add continuous deliver to your project.

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

You can check it out for yourself at gocd.org/sedaily. Thank you so much to ThoughtWorks for being a long-time sponsor of Software Engineering Daily. We're proud to have ThoughtWorks and GoCD as sponsors of the show.

[END]