EPISODE 319

[INTRODUCTION]

[0:00:00.9] JM: In Bitcoin, every transaction in the shared ledger has the sender, the recipient, and the value. These are different fields that are on every line of a transaction. This ledger gets appended infinitely and is shared within a peer-to-peer network.

Zcash is a cryptocurrency with all of the features of Bitcoin. In fact, it's a fork of Bitcoin. Plus, it has encrypted transactions. The sender, the recipient, and the value fields are all encrypted. If Bitcoin is "http", Zcash is like "https"; it's a secure transport layer.

Nathan Wilcox works on Zcash, and in this episode we discussed why an encrypted version of Bitcoin is useful, how mining works, and how Zcash, the company, is structured. Nathan also gives some context for the current state of the Bicoin and cryptocurrency community and where Zcash fits in.

[SPONSOR MESSAGE]

[0:01:11.9] JM: Release the Kraken! GitKraken, that is. Are you tired of feeling like you're sailing the stormy seas, because you have a clunky, old Git user interface? Unleash the beast, that is Axosoft's GitKraken. Voted 2017s most popular Git GUI for Windows, Mac, and Linux.

GitKraken is designed to make you a more productive Git user. The app offers efficiency, elegance, and reliability. The UI equips you with a visual understanding of your branching, merging, and commit history, and features multiple profile support, one click undo and redo, a built-in merge tool, and fast search.

Run the installer, open the app, and set sail with GitKraken. Easily setup integrations with GitHub, GitHub Enterprise, Bitbucket, and GitLab. That's one high performance sea monster. Visualize your version control and code on into the sunset sailors. Visit gitkraken.com/sedaily and use promo code "sedaily" to get $10 off GitKraken Pro.

[INTERVIEW]

[0:02:34.9] JM: Nathan Wilcox works on Zcash. Nathan, welcome to Software Engineering Daily.

[0:02:39.8] NW: Hi. It's great to be here.

[0:02:42.0] JM: This podcast is for software engineering generalists. I'd like to start at a high level, and then we'll go deeper into Zcash. Everybody who is listening to this podcast knows what Bitcoin is. They have a basic understanding of the shared ledger system. Could you give the listeners a brief reminder or explanation of why the idea of a financial blockchain is a fundamental breakthrough in computer science?

[0:03:10.5] NW: Sure. I think the breakthrough of Bitcoin was in providing an internet supported currency that isn't controlled by any particular entity. It's governed by a set of rules that aren't clearly defined, and then people can opt in to following those rules and using the system, or not, at their discretion.

I think the key part of the design that was surprising to many people like me was how well it balances sort of protocol design as well as incentives so that they kind of reinforce each other.

[0:03:48.0] JM: The most exciting thing to me about cryptocurrencies since I started reading about them is micro-transactions, the idea that you could send somebody in Nigeria, a penny, with almost no transaction cost, is huge, and this is something that we can get to eventually. We're still a ways away from it, but I think it's important to keep in mind these higher level applications that we will get to, because right now there's a widespread perception that people who work on blockchains are either obsessed with privacy, or they're an archaic libertarians, but there's actually just raw utility in blockchain technologies.

What are the biggest breakthrough applications that you're looking forward to that keep you working on cryptocurrencies day-to-day?

[0:04:40.0] NW: You brought up micro-transactions, so that's on my mind now. I am really excited about potential there. I'm really excited about the Brave browser, which is an example of a use of a kind of micro-transaction. That's an example of changing the whole publication incentive model for the web. If it's successful, it could change the way the web is for many people.

Another technology I'm interested in is smart contracts, and I think it's because I envisioned that enabling new kinds of uses that aren't even in the public consciousness yet.

[0:05:23.2] JM: Right. Yeah, and we'll get into that. We'll get into the smart contract application. I'm particularly interested in what Zcash enables with regard to smart contracts. Let's continue with a little bit of history and context. Zcash was founded by your brother Zooko, who had worked on cryptocurrency related stuff since the 90s. What kind of discussion did you have with him when Bitcoin came out and started to gain traction, because I'm sure he was excited about it then. What were the conversations you were having with him back then?

[0:05:56.5] NW: Yeah. When I recall conversations about cryptocurrency, I remember a time before I had heard about Bitcoin when I had discussions with my brother, Zooko, and some other folks, just friends, about the potential to have an internet governed currency.

I remember the first time I heard about Bitcoin, it was in a discussion with a group of folks out to dinner and Zooko was there, and one of my friends was really excited about it in describing it. I asked Zooko if he had heard about, and he said, "Yeah. Well, it seems kind of interesting, but it has this strange consensus thing, and I'm not so sure I like that." It didn't fit his sort of design philosophy. That's the first comment I remember hearing him make about it.

Pretty quickly, within a couple of weeks, or a month or two, it kept coming up in conversations between us and also with other friends. It's sort of — From my perspective in my community, it sort of overtook the community like a wildfire, your particular waiting time, where everyone was talking about. In fact, I remember being on a discussion board to go to a hacker camp called ToorCamp, and people were arranging rides. One of the ride carpooling things had a list of rules, and the last rule was, "No discussions about Bitcoin on this drive please." That was like, for me, an indication of the times how much excitement there was.

[0:07:37.6] JM: Why did the consensus protocol seem implausible at the time?

[0:07:41.9] NW: Yeah, that's a good question. I think a lot of people — It took them a while to wrap their heads around, and maybe for some people, they still haven't — I think some people gave up and just sort of wrote Bitcoin off. For the people who stuck around and for the network itself, it's obviously working, because it's many years old without any major design disasters.

[0:08:08.5] JM: Yeah.

[0:08:09.5] NW: I think one thing that may trip people up is that the selection of the winning block seems so random. That's actually a valuable quality. In a first description, like if I'm talking to nontechnical friends, it just seems kind of crazy that you would follow a random stranger's advice about what should be in the ledger. It just doesn't seem like that could possibly work.

[0:08:37.0] JM: It's funny, it's just one of these things that, at scale, it makes a ton of sense. In small sample sizes, it looks sort of crazy. At scale, it averages out to making sense.

[0:08:49.4] NW: One other aspect to that that I think trips a lot of people up is the incentives, like, "Why should I use this block that a stranger told me about?" It's a sort of a self-fulfilling prophecy, it's because everyone else will, because those are the rules that they're following, and because you know people are following those rules, that's why you will follow the rules. They're sort of these almost circular seeming reasoning that trips a lot of people up in my experience.

[0:09:18.3] JM: What are some of the important features that Bitcoin has been unable to implement? Obviously, we've seen Bitcoin has gained traction, but, clearly, there is room for other cryptocurrencies. What are the important features that it hasn't been able to implement?

[0:09:36.7] NW: I guess the Zcash party line is that it lacks fungibility, which is intimately connected to privacy. It's possible that it may be able to implement improved privacy, and we've seen a lot of auxiliary improvements, protocols like CoinJoin which don't require poor upgrades to the Bitcoin protocol, but which people can build on top of Bitcoin.

[0:10:05.0] JM: You mentioned fungibility. Zcash is a fungible cryptocurrency, and we'll start to get into Zcash here. Fungibilty means that each coin has the same interchangeable value as any other coin. Why doesn't Bitcoin have fungibility, and how does Zcash gain that property?

[0:10:25.6] NW: Right. Bitcoin does not have that feature, because anytime you receive a Bitcoin, the way you can verify that that's valid amount of value is by tracing its history through all time and iteratively verifying, at each step, the transfers were valid. That gives you a view of the history of all coins and the history of all transactions. You may want to distinguish between those histories. Two people might each send me one Bitcoin, but I might prefer one of those Bitcoin more than the other because of its history.

[0:11:09.6] JM: Interesting. To give people a sense of what Zcash actually is, we kind of passed over this, it's a superset of Bitcoin. You forked all the code in Bitcoin and added encryption to the transactions. In Bitcoin, every transaction in the ledger has, basically, three fields. There's the sender, the recipient, and the value. This ledger gets appended infinitely. Every time there's a new transaction, you add sender recipient value and it gets shared in the peer-to-peer network. Zcash is the same thing, except you encrypt the sender recipient and value. Explain why that's useful.

[0:11:53.4] NW: That description is pretty high level, and I think that captures the essence. If you — There's a subtlety there, which is that if you're receiving a coin, you don't know anything about it, because of this encryption. All you know is the amount. If the sender chooses to send along a message, what we call a memo fill, they can do that.

That's all you know in band about that transfer. This is how Zcash provides the property of fungibility. If you want to, you can make decisions about receiving that coin based on the context, you're receiving based on who's sending it to you, or any other information you have, but the coin itself has nothing — No information attached to it. It's just an arbitrary value.

[0:12:45.2] JM: Encrypting the sender, the recipient, and the value, why is this hard?

[0:12:52.2] NW: Yeah, this is hard, because if you know a bit about blockchains and you know a bit about encryption, you can realize why this is hard, because blockchains work by having all of

the miners and all of the participants verify that all of the transactions are valid. In Bitcoin, they can do that by seeing all of the details. The only secrets are the private keys users control in order to control spending of their funds. Those obviously don't appear on the blockchain.

Here, with Zcash, we want to have these details verified by everyone, because we still want it to be open and decentralized, but we don't to reveal the details to people who are verifying the blockchain unless they are the ones receiving the transactions.

If you're familiar with basic kinds of encryption, like asymmetric public-key encryption, or symmetric encryption, neither of those by themselves can give you what you need for Zcash. We use a new kind of technology called zero-knowledge proofs that provide that for us.

[0:14:07.0] JM: I think I was at a — I was at a Zcash event. I think it was the launch of Zcash in San Francisco. I forgot what the name of it was, but I'm pretty sure that Zooko mentioned that he doesn't even really understand how zero-knowledge proofs work, because they're extremely complicated. Can you give a high level explanation of what is zero-knowledge proof is, why this is a useful abstraction?

[0:14:31.9] NW: Yeah. I can give a high level overview, because my understanding is also at some level. At some point, there's a block box for me. Fortunately, we have an excellent team, so I can rely on people to understand all parts of the stack.

The high level overview is that you can construct a logical statement about some inputs and then you can do two processes once you know the statement. One if you can generate a proof, and one is that you can verify a proof. When you generate a proof, there's an output that's like an opaque blob to me, a string of bytes.

If you take the string bytes and the public inputs and hand those to anyone you want, they can run the verification of the statement with the public inputs, and even though they know nothing about the private inputs, if the verifier succeeds, they know that the statement is true for all of the inputs. That gives you a pretty general building block for all kinds of things.

[SPONSOR MESSAGE]

[0:15:53.1] JM: Good customer relationships define the success of your business. Zendesk helps you build better mobile apps and retain users. With Zendesk mobile SDKs, you can bring native in-app support to your app quickly and easily. If a user discovers a bug in your app, that user can view help content and start a conversation with your support team without leaving your app.

The conversations go into Zendesk and can automatically include information about the user's app information, device information, usage history, and more. Best of all, this is included with Zendesk for no extra charge. Use the out of the box iOS UI to get up and running quickly, or build your own UI and work with the SDK API providers. Keep your customers happy with Zendesk.

Software Engineering Daily listeners can use promo code "sedaily" for $177 off. Thanks to Zendesk for supporting Software Engineering Daily, and you can check out zendesk.com/sedaily to support Software Engineering Daily and get $177 off your Zendesk.

[INTERVIEW CONTINUED]

[0:17:20.9] JM: Right. Now, one of the phrases that I read on the website is if Bitcoin is like http, Zcash is like https. It's a secure transport layer. Why did you need to build an entirely new cryptocurrency if all you needed was a secure transport layer?

[0:17:42.4] NW: That's a great question. I think in principle, it would be possible to upgrade Bitcoin to have these kinds of features. In practice, Bitcoin and all cryptocurrencies are a big emerging ecosystem with many different stakeholders who want different things and have different priorities.

In fact, I believe, Matthew Green, one of the scientists who developed the Zerocash paper, which is — Zcash is basically an implementation of the Zerocash research. I think he had conversations with Bitcoin developers and proposed augmenting Bitcoin developers and proposed augmenting Bitcoin, and I think that consensus at that time was because it's a new kind of technology, it would be better to have it proven sort of independently as a separate

system. Then, if it — In the long run, if it seems very stable and mature, maybe Bitcoin could adopt it. Yeah, that's the route it took.

[0:18:44.4] JM: Oh, okay. Does Zcash mining work the same as Bitcoin mining works?

[0:18:50.0] NW: At a high level, it's the same, where it is a proof of work consensus mechanism, but the kind of work is different, so we use a different algorithm besides SHA256. We use an algorithm called Equihash, which is a memory-hard hashing algorithm. Ideally, the constraining resource for Zcash miners should be RAM rather than compute power.

[0:19:19.2] JM: Why that desire to make RAM the limiting gradient rather than compute power?

[0:19:26.5] NW: We wanted to change the proof of work, because we didn't necessarily want existing Bitcoin miners to be able to dominate the Zcash mining network, because they have scaled up vertically and they have lots of capital invested in that now. What that means is if we just reuse the same proof of work, even relatively small, Bitcoin mining operations would be able to have a huge impact on the Zcash network when it was young.

In the long term, if all — Basically, it would put us in contention with the Bitcoin network mining system. We didn't like that. Since we wanted to change it, we also thought a little bit about, I guess, the economic, or the systemic goals. Our thinking that time was that in Bitcoin, by this time — And Bitcoin, it was already at the case that there were specialized ASICs circuits developed to mine Bitcoin. What that meant was there's sort of a closed loop between ASIC design manufacture and actual mining operations, where if you're the first to develop an ASIC, you capture a larger fraction of the mining capacity, so you have a larger revenue and you can invest more of that revenue into improving the next generation of the ASIC. There's this feedback loop that makes it difficult for new entrance into the mining market.

We wanted to see if we could mitigate that somewhat, if possible, and we thought if we could develop the mining systems so that the limiting factor, in terms of capital investment, was just general purpose RAM, that it would reduce the amount of advantage large Zcash miners had over new entrance, because the assumption is that they won't be able to make any sort of

devices that are much better than general purpose RAM. We wanted to lower the barrier to entry to new miners, basically.

[0:21:44.5] JM: Sure. Makes sense. Zcash is a superset of Bitcoin as we have said. It's Bitcoin plus encryption, sort of at the very reductive level. In what ways is the lack of encryption a feature, because — In some ways, there's no way a miner is saying Zcash hasn't made Bitcoin obsolete. Why is that? At a fundamental level, what differentiates Zcash from being just superior to Bitcoin?

[0:22:19.7] NW: I feel like there's almost two questions there, because one is kind of specific to Bitcoin itself, and one is more about having transparent transactions, or transparency in transactions.

Let me talk about the transparency first. If you have encryption, it's always possible to reveal secrets at your discretion. That's why, in Zcash, we talk a lot about selective transparency, or selective disclosure, where the idea is users can go ahead, and if they want to, reveal details about transactions. They can still achieve some of the similar benefits you get from having a completely transparent blockchain. Some people really love that aspect of Bitcoin, the fact that there is that transparency. You could have nonprofits, or whatever that the public can audit. How they're spending their funds, for example.

The other question sounded to me kind of like if Zcash is superior to Bitcoin, then why isn't — Why is Bitcoin still around? Is that how you would —

[0:23:29.1] JM: No. I wasn't asking that. It was sort of like I understand that there are some fundamental difference. It's not necessarily like Zcash is a superset of Bitcoin, meaning it has all of the positive aspects of Bitcoin. I think even just the fact that Bitcoin has been around for a while and is widely accepted. Even if you just take like brand recognition, then you have some degree of qualitative — Some qualitative difference there, even if it's — Even if you say like, "Oh! Zcash has feature parity and more." The brand difference makes the difference. I was basically getting at the question that you answered, which is that sometimes you want transparent transactions. You don't always want encryption.

I want to talk about some other stuff in the ecosystem. Now that we've touched on the kind of relevant aspects of Zcash that will let us have a conversation around it. Ethereum is the other cryptocurrency that has gained the most traction aside from Bitcoin. It allows for a touring complete set of operations so that you can use it to build smart contracts. What kinds of smart contracts will people be able to broker using Zcash?

[0:24:48.2] NW: Currently, in the current form, you can do anything you can do with Bitcoin script, which is more limited than what's possible with Ethereum smart contracts. In the future, we'd like to change that, or I would like to change that so that it's possible to do more sophisticated kinds of smart contracts. Maybe similar to Ethereum, although I would — I think I would advocate for some differences in the design of the smart contract platform, but maybe that's getting into weeds. I'm not sure.

[0:25:19.6] JM: What I was kind of curious about is can you use the Ethereum smart contract platform, but use Zcash to pave for those smart contracts. Do they integrate with each other?

[0:25:32.3] NW: We've been collaborating with Ethereum developers to have various kinds of integration. In some sense, yes. I could step back and say, at a broad level, all of the cryptocurrencies can interact in a way that's more streamlined or maybe more surprising to people from traditional financial technology industry, because since it's possible for anyone to just download and deploy any of these systems, it's really easy to deploy systems that integrate different blockchains.

Once you start zooming in on ways for blockchains to interact, there's a lot of stuff going on there. There's also another question. I wondered if you were asking about if we could take a step back and sort of merge Zcash and Ethereum, or make a new system and sort of cherry pick features, what would we want for that new system.

[0:26:33.6] JM: Sure, you can answer that question.

[0:26:37.2] NW: Yeah. If we start with Ethereum and port some of the Zcash privacy technology to it, there are several different ways you can do, and a simplistic way would be to provide the

ability to do zero-knowledge proving on the Ethereum platform, which it seems like the Ethereum community is interested in doing.

I think that would be great and would have great benefits, but I also think that, in the end, with that sort of approach, the platform will maybe have different kinds of smart contracts, and each contract itself will have some kind of internal privacy. Maybe there's one contract for an embedded currency, say, and another contract for a voting system.

The interactions between those two are sort of in separate privacy domains. For example, I could look at the blockchain and I could see that this particular client is interacting with the voting contract and not the sub-currency contract. I would learn something about what that client is doing.

I think the holy grail for a smart contract system that uses zero-knowledge proving or other kinds of privacy technology would be one in which you have some features and guarantees about smart contracts, such as they can interact, or the ordering of transactions for a given smart contract is well-known and well-ordered, or there might be some of those features that you want. In addition, when people are interacting with any of the smart contracts on the platform, they have the same level of privacy. Sort of the whole platform is protected by one monolithic privacy shield. That's kind of the holy grail. I don't know —

[0:28:34.8] JM: Anonymized smart contracts.

[0:28:36.9] NW: Right. I guess the difference is between individual smart contracts that have their own privacy protections, or a platform where all of the contracts share the same privacy features.

[0:28:52.1] JM: I did notice that the domain name Zethereum has been taken already.

[0:28:57.8] NW: I didn't know about that. Yeah, I think a lot of people are — I think a lot of people are excited about this idea.

[0:29:04.3] JM: Yeah, me too. Banks and financial institutions are getting into blockchain technologies, the uptick. There's been an uptick. We've had ripple for a while. There's also chain.com. I think the chain.com CEO is an investor in Zcash. What are the opportunities for financial institutions in blockchain technologies? Also, in Zcash specifically, are banks going to want to use Zcash?

[0:29:36.9] NW: That's a huge question, and it's a complex question. I think that financial — The traditional financial industry will end up using blockchain technology. What blockchain technology they end up using will be interesting to see and how we get there, because I believe, currently, the status quo, as I understand it is that they're really interested in blockchain and different people say different things like, "The blockchain, or just blockchain is a mass noun, or whatever."

They're interested in this word, and there is kind of a fledgling industry of companies that focus on creating blockchain solutions for the financial industry, and there's a lot of interest within the financial industry, like their own in-house initiatives and investigations.

What blockchain means is — It depends on who you ask. I think, in some sense, the state of things right now is they want to discover why there's all these hype about this thing and they want to figure out how they can use it. I think that they are very weary of using public open permission with blockchains. I think it's because they don't quite get blockchains yet, because the amazing thing about Bitcoin is that it demonstrated you could have rules that restrict and limit how users can use the system, but there's no entity, there's no single entity that; A, defines the rules; or B, enforces the rules.

The enforcement is done by the participants and miners of the blockchain, and that's pretty uncomfortable, I think, for financial institutions to wrap their head around, because they're used to — If you want to enforce a set of rules about how transactions occur within your institution, then you operate the transaction system and you handout access to the transaction system to the right participants. If they don't do the right thing the right way, you deal with it in each case, right?

[0:32:01.7] JM: What's so massive about blockchains is the same pressures that will push down the cost of microtransactions. Right now, if you want to send a penny to Nigeria, you've got to pay a transaction cost that is so onerous, it totally overshadows the penny transaction. Those pressures will benefit financial institutions, because you just get away to send money around for cheaper, because it's on blockchain.

I could imagine Zcash. I'm not sure if you would want to say, "Hey, I'm letting Wells Fargo make my encrypted transactions, or something." I'm not sure that's how it'd manifest. I could see it being useful for banks to make client-destined transactions between each other, maybe. I don't know. Does that sound plausible?

[0:32:51.6] NW: Sounds plausible to me. I wouldn't call them client-destined, because I think business needs privacy legitimately to be competitive with competitors —

[0:33:01.5] JM: Oh, yeah! I don't mean client-destined in any sort of negative context.

[0:33:05.2] NW: Oh, okay. Yeah, I can see — I guess the vision I see is that, first of all, for a bank to deploy a blockchain thing, it doesn't make too much sense if they're just an institution running a thing that tracks transactions, because, in that case, you could just have a database that manages those transactions and it would be much more efficient.

Blockchains become interesting when you have multiple institutions interacting, or users from multiple institutions interacting, and you want to — There are several benefits, but one is just keeping all of the records consistent to a given set of rules, which is exactly what Bitcoin is good at doing. Also, outsourcing — Potentially, outsourcing management or maintenance of the ledger in a way that this is sort of distributed, so it doesn't require everyone accessing the system through a particular hub, or particular gatekeepers.

Those might be ways in which the financial industry is sort of gets in the blockchain with various products that are operated by consortiums or sort of like clubs where financial institutions join. I suspect, or I wonder, if in the long run, there's sort of a networking effect where fewer blockchains is easier to interact with. At some point, you might have this blockchain that's operated by a consortium of banks so that they can do transfers between each other efficiently,

but their customers might be using Zcash, or Ethereum, or Bitcoin and they want to do — There's going to be this extra hop, or this extra bridge. At some point, I wonder if they will breakdown and just start offering direct support to the public blockchains, or if it will always be sort of this compartmentalized federated kind of blockchain world.

[SPONSOR MESSAGE]

[0:35:11.9] JM: You are building a data-intensive application. Maybe it involves data visualization, a recommendation engine, or multiple data sources. These applications often require data warehousing, glue code, lots of iteration, and lots of frustration.

The Exaptive Studio is a rapid application development studio optimized for data projects. It minimizes the code required to build data-rich web applications and maximizes your time spent on your expertise. Go to exaptive.com/sedaily to get a free account today. That's exaptive.com/sedaily.

The Exaptive Studio provides a visual environment for using backend algorithmic and front-end component. Use the open source technologies you already use, but without having to modify the code, unless you want to, of course. Access a k-means clustering algorithm without knowing R, or use complex visualizations even if you don't know D3.

Spend your energy on the part that you know well and less time on the other stuff. Build faster and create better. Go to exaptive.com/sedaily for a free account. Thanks to Exaptive for being a new sponsor of Software Engineering Daily. It's a pleasure to have you onboard as a new sponsor.

[INTERVIEW CONTINUED]

[0:36:41.9] JM: Let's talk about Zcash, the company, which is what you work for. You're a project manager for Zcash, the company. What does the company do? We've been talking about the open source project.

[0:36:54.9] NW: Right. The company develops the software right now. We're the main set of developers, although it's encouraging to see some community contributors getting involved. Also, it's exciting to see different cryptocurrency services, like wallet providers, or exchanges, et cetera, integrate Zcash. Right now, the main development effort is housed within our company.

We have a big engineering team, and that's most of our company. We also have the science team. There were seven scientists who invented the zero-cash protocol and they are all partners in that company, and we collaborate. They do research that's relevant, sometimes, to Zcash, and we sort of like have a feedback look going where we describe futuristic things we think would be great. They describe research they're doing that could be useful for Zcash. That's the basic structure right now.

[0:38:02.9] JM: Most of the companies that I talk to are web-based businesses with a business model that's pretty easy to explain. There are aspects of these companies that are almost always the same. They run on AWS, or Google Cloud computing engine, they have a continuous delivery workflow. They organize into two pizza teams.

When you're building a cryptocurrency, what are the characteristics of the typical company that go out the window? What is different about building a cryptocurrency company?

[0:38:39.0] NW: That's a great question. First of all, I think, for us, we — I'm speaking from sort of the engineering and startup side of Zcash rather than from the scientists' perspective. From my perspective, entering into this collaboration with the scientists, I saw the engineering task as kind of a well-defined thing. Basically, what we are doing is kind of like a fast follow sort of thing, because we already saw that Bitcoin was operating successfully and it already had a working design. Then, these scientist came up with this excellent improvement, and so our plan is just to join those two things. That's like step one. That's a very clear goal.

Because that was our first goal, we didn't necessarily do the kind of market research, or quick iterations on a minimum viable product that I often think of startups as doing, at least for that initial phase up to our launch.

[0:39:50.1] JM: Okay. I want to zoom out a little bit. We had Rusty Russell from Blockstream on the show to discuss sidechains and micropayments and how these exchanges between different cryptocurrencies might work. Does Zcash share the same set of beliefs about the future of cryptocurrencies as the broader Bitcoin ecosystem?

[0:40:19.9] NW: I'm not exactly sure what those beliefs are.

[0:40:25.6] JM: Okay. It's probably a poorly formed question.

[0:40:28.6] NW: My understanding of one set of beliefs is that sort of from the sidechain's camp, I guess I would call it. Maybe that's what you're describing, is the broader Bitcoin community?

[0:40:38.8] JM: Yeah, that's the way I should have phrased it.

[0:40:40.7] NW: Okay. I think I —

[0:40:41.9] JM: Sidechains and lightning networks.

[0:40:44.0] NW: Right. Okay. The view for sidechains is one where there are many different kinds of technology platforms that make different tradeoffs or have different advantages, but they all have a shared unit of value sort of spread among them and streaming through them. The vision there is you can take — We could keep Bitcoin kind of stable and secure without doing anything risky to its design. Then, people can come up with experimental wild ideas, like zero-knowledge proofs and deploy a new platform that implements that.

Then, people who hold Bitcoin, if they want to use that, can transfer that into this new system, interact there. Then, if they want to, they can transfer back into the core Bitcoin platform.

I think that I generally share that vision, and I think that the — The devil is in the detail, like the nitty-gritty of different mechanisms that transfer value between systems and how systems are coupled is where we might see things differently. I think one big difference of opinion I have — I might change my mind about this. Currently, to me, I like to see slightly less strongly coupled systems. For example, I'm happy with Zcash being an independent blockchain and Bitcoin

being an independent blockchain and then sort of streamlining the ability for individuals to exchange Bitcoin for Zcash and vice versa.

In this sort of vision I'm promoting, the user experience might be like you have a Zcash wallet, or a Bitcoin wallet and you go to a store and they only accept the other thing. You have Zcash, the store only accepts Bitcoin, but it's no biggie, because the wallet just uses some technology that makes an exchange efficiently and quickly, and so you just are shown a price in maybe some third currency, like dollars, and you just click yes. Maybe it has a little indication of the fee that you might incur from exchanging.

Whereas, I think in the sidechain vision, at least as I understand it, I might be oversimplifying it, but it would be the user experience is sort of like you use a Zcash wallet, because you want privacy, but in it, is stored Bitcoin, and you go to store, and the store accepts Bitcoin, and everyone uses Bitcoin.

The difference between those two views, in my opinion, is that to do sidechains well, the blockchains themselves have to have a kind of coupling, which means there needs to be at least some amount of consensus between nodes operating the two networks to integrate with the other networks. Then, the question for me becomes — There's sort of a governance issue I see, and there's also a user choice thing, where it's like if I'm using Bitcoin and somebody says, "We're going to couple it to Zcash," but I'm a Zcash skeptic and I'm like, "No! Wait! That's really dangerous." What happens is Bitcoin goes ahead and does that? Does that mean I begin to value Bitcoin less because it seems less stable to me than it used to?

Meanwhile, another user might love Zcash. I guess I should be the user who loves Zcash and we could — Anyway. They think that's great. There might be this governance issue. Also, the choice doesn't seem — For that coupling, isn't an individual choice. It's sort of a choice for the network. Whereas, if there's — Basically, I like independent user choices. If one user likes Zcash a lot and doesn't like Bitcoin at all, they can just store all of their value in Zcash and just use Zcash stuff. If they need to interact with Bitcoin, they do whenever that need arises.

[0:45:01.6] JM: Interesting. Just to wrap up, I'm also curious about the company 21. This is a company that's been heavily financed. I know they're building some technology around mining

Bitcoin. They seem to have a vision of you have a chip in your refrigerator and in your toaster and these things can mine Bitcoin, because since you're going to have a chip that's sitting in your IoT devices and they're doing nothing half the time, or more than half the time, maybe you might as well mine some Bitcoin. What do you think of this company 21?

[0:45:36.7] NW: I think that's an exciting vision. I don't know — It remains to be seen how it pans out. I think it would be interesting if mining was defused into all consumer products. I would definitely —

[0:45:53.5] JM: Certainly be better than a status quo.

[0:45:55.5] NW: Yeah. I guess I am a little bit skeptical. I guess there's a couple of arguments for how that could work, but one is I'm skeptical that that could supplant or replace the existing Bitcoin mining network just because I think there is so much economy of scale and specialization that goes into that, that it's hard for me to see miners being outcompeted in that way. I just assume diffuse mining in consumer electronics couldn't ever reach the same sort of mining capacity.

The more interesting or compelling part of 21 story I've heard is that what this would allow is that these devices would accrue Bitcoin just naturally. There would be money sort of appearing on all of these different devices, even if it's a tiny, tiny amount, and then that can sort of bootstrap ways for them to interact through micro-payments or whatnot — Smart contracts. That's an interesting vision.

It would be exciting if things moved in that direction. It would be a little terrifying for me, personally, because — I don't know. The Internet of Things, I find kind of terrifying just from a security angle.

[0:47:09.2] JM: The IoT story — The thing is the IoT is coming and it's going to be a security problem whether we like it or not. I would rather have some company that is distributing chips that are built in a way that is secure from the ground up rather than having just total bedlam in terms of what the devices look like.

I had a conversation with somebody recently about how android — I guess there's an Android IoT version of the Android, and this is what Google's play on IoT is going to be. I find that somewhat reassuring that, "Oh! They've got a version of Android that they're going to deploy for their IoT devices or for people who want to build IoT platforms." That's great. I would love to have a standardized operating system rather than just having these Linux distros with the same username and password all over it.

[0:48:05.4] NW: Right.

[0:48:06.4] JM: That's the scary part.

[0:48:08.3] NW: Yeah. There's a whole topic I'm interested in, which is how — We've talked a bit about micro-payments and I mentioned Brave browser, and I think I often — Maybe other people often imagine use cases that are sort of like analogies for what we currently do with money. You put a quarter in the slot machine in order to go through the turnstile kind of thinking.

I'm actually really interested in sort of a computer science area or research, which is if you're going to be designing a new protocol and at your disposal, you have the ability to do these smart contracts, or micro-payments, or things like that. How does that change considerations, like, security, for example, if you want to have a webcam and it's going to connect to the computer and the webcam just requires a thousandth of a cent transfer in order to initiate that connection, then that would inhibit internet-wide scanning of these webcams, because that would become prohibitively expensive. I'm really curious about how these new technologies will open up new areas in design space in addition to maybe just porting over our current turnstile style thinking.

[0:49:35.2] JM: Certainly. Even in just the turnstile subscription based transactions, there is a lot of ground to be covered. I've done a lot of shows about the advertising fraud ecosystem and basically how most — The average person really under — Even the average software engineering really underestimates how bad advertising fraud is and how much trouble it creates, how it incentivizes things like fake news, and botnets, and it's just this tremendous problem that people underestimate. You see Medium as a leading indicator moving toward — Medium, and like — Patreon type models, or just like old school subscription models, I guess. This is where I

think a lot of the best content is going to be behind, is some sort of subscription based model. When we have more widespread adoption of this in our protocols, I'm sure that's going to permeate to the user level as well.

[0:50:36.2] NW: Actually — Yeah, I'm in love with the idea of subscriptions for content. It's funny, I was just realizing, I hate pay-walls. The thing is I think the only reason I hate pay-walls is I don't want to give my email to anyone else. I have already given it out too many times, so I get all these spams.

[0:50:54.8] JM: It's the experience.

[0:50:57.0] NW: If I could pay without having to sign up for anything, if I could just click to read an article, I almost likely — It's almost certain that I would do that often.

[0:51:09.2] JM: Yeah. Okay. Nathan, I want to thank you for coming on Software Engineering Daily. I'm excited about Zcash, and I'll be watching it closely.

[0:51:16.4] NW: Cool. Thanks. It's been great to be here.

[END OF INTERVIEW]

[0:51:24.3] JM: A few quick announcements before we go. Software Engineering Daily is conducting our annual listeners' survey, which is available on softwareengineerigndaily.com. You can click on the survey link. The survey really helps us understand our listeners and give us data that we can show to advertisers that help get us better sponsorship deals.

Also, the Software Engineering Daily community has started working on Mineranker. This is an open source newsfeed platform. We are trying to democratize the idea of a newsfeed so that the only newsfeeds in town are not necessarily Twitter, or Facebook, or any other centralized newsfeed. We'd like to make it possible for anybody to make a newsfeed.

You can check out the Mineranker Project at mineranker.com. You can check out and implementation of Mineranker at softwaredaily.com. You can find links to all of these stuff at

softwareengineeringdaily.com. There, you can also find a link to join our Slack group to follow us on Meetup for future meet ups and other information.

Thanks again for listening.

[END]