EPISODE 536

[INTRODUCTION]

[0:00:00.3] JM: For the last decade, Bitcoin's proof of work system has run without disruption. In a proof of work scheme, Bitcoin miners compete to solve a cryptographic puzzle associated with a block of transactions. Every 10 minutes, all the Bitcoin miner nodes race to be the first to solve a block of transactions. Only one miner wins each block, meaning the other nodes' time was ultimately wasted. There is also a massive expense of electricity.

Bitcoin is a system with low transaction throughput. It's about seven transactions per second. Computer scientists have wondered is there an alternative way of doing consensus? What if we took all of the wasted compute power from proof of work and allocated in a way that makes transactions get processed faster?

Unfortunately, Bitcoin's governance tends to be extremely conservative. We can't run this experiment on Bitcoin. A change to the consensus mechanism probably won't happen anytime soon in Bitcoin, unless you count Lightning Network and side chains.

Ethereum's consensus mechanism is modeled after that off Bitcoin, its proof of work mining. Ethereum's governance ethos is quite different. Ethereum is in the process of planning and implementing proof of stake, which is an alternative consensus mechanism, in which trusted validators are chosen to validate blocks of transaction.

Subhan Nadeem is a student at the University of Waterloo, where he studies computer science and business. He's the author of several popular articles on Medium that explain blockchain concepts. He joins the show to talk about crypto from the point of view of a student, and he also gives us a great and thorough walkthrough of some different consensus mechanisms.

If you like our series about cryptocurrencies, you can find all our old episodes by checking our apps in the iOS or Android app store, and they have all 700 of our episodes. We've got recommendations, related links and discussions and more. It's all open source. If you're looking for an open source project to contribute to, we'd love to get your help.

You can go to github.com/softwareengineeringdaily. We welcome all kinds of contributors, new developers and experts and engineers, as well as non-technical people, like if you're in marketing or sales or design. Actually, those are technical roles so I should specify this more specifically, but it's an open source project where we aren't just looking for engineers, we'd love all kinds of commerce. If you're interested in getting involved in the SE Daily open source project, we would love to have your involvement.

With that said, let's get to this episode.

[SPONSOR MESSAGE]

[0:02:46.1] 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]

[0:04:29.3] JM: Subhan Nadeem, you are a student at the University of Waterloo. You're studying computer science in business. Welcome to Software Engineering Daily.

[0:04:36.3] SN: Thank you very much for having me, Jeff. I'm a huge fan. I've been listening for a while and I'm very glad to be here.

[0:04:41.3] JM: Well, that's great to hear. I'm a fan of your Medium work, so the respect is mutual. I want to start off with some basic questions about who you are and your circumstances, because I am doing this month of shows about cryptocurrencies and related technologies. I'm trying to get an understanding not just of the technology, but the community and who is adopting it, who is paying attention, why they are paying attention, the different motivations of people. Let me just ask you as a student. What's your perspective on the question of why engineers should look closely at cryptocurrencies?

[0:05:19.8] SN: Absolutely. That's such a really good question, because – like you mentioned, I go to the University of Waterloo. My interest in blockchain technology and Bitcoin technology actually stems from the environment in which I study in. About six months ago when everything started to get into a frenzy, blockchain technology was the buzz word and it still is. Especially in Waterloo which is described as the Silicon Valley of Canada, things started to really take off, they started buzzing about blockchain technology, companies started popping up everywhere.

What's happening now is that it turned into this industry right for opportunity. Everywhere you look, you're seeing blockchain technologies popup, you're seeing blockchain researchers, blockchain learners, educators popup. Really, I think what's important to realize for anybody looking to get into this field, they're trying to fund the – realize the value in this field is that this technology itself, blockchain, Bitcoin, Ethereum, all of these platforms, they're largely untapped.

We're almost 10 years in, but the true potential of all of these have not been realized. To really understand why that is, you really have to get into the nitty-gritty and the fundamentals of the technology. That's where I started myself when I got into trying to realize the potential of this technology. I told myself, you can't really understand what's going on here without understanding the fundamentals. It's a tough question to answer without explaining why this

technology is as valuable as it is. That hype is not unwarranted and it's existed for the last year or so and it's going to keep going.

[0:06:53.6] JM: Right. This is one of the reasons that led me to eventually deciding I really needed to dive deep into it was to do anything short of a dive into the fundamentals is to honestly do – the service to yourself as an engineer, because it's really hard to understand the significance of the technology without really diving in and understanding the bigger picture and seeing everything.

You risk ending up as a victim of some sound bite like, "Oh, I'm excited about the blockchain, but not Bitcoin," which does not make any sense. I mean, it makes sense in the sense that private blockchains are cool, I guess in the sense that you could have a centralized but partially exposed ledger.

Really the meat of what makes this stuff important is what is at the extremes of the technology, the extremes of the decentralization, even if that's not what ends up being what is most widely used, or what is most widely impactful. Just seeing the extreme end of it is really the only way to understand the potential of it, from my point of view at least.

[0:08:06.6] SN: Absolutely. I agree. Two things that always come up in common conversation is one, nobody really understands what Bitcoin is. Everybody talks about it. I see that as a challenge to myself. I mean, I'm only a student. I'm still in school, but hey, I mean if I can spend a couple of months researching it and understand the fundamentals of the technology, I feel like anybody can and should be doing so without jumping into the batwing, like you said talking about private blockchains.

Yet, now realizing the true proof of concept that came to life with Bitcoin and how it's being moved forward with platform such as Ethereum and other platforms such as private blockchains as well. Truly understanding how private and public key cryptography, one-way hashing and as well as distributed – the distributed ledger system that involves blockchain technology, how all these systems come together without realizing that I feel like is very difficult to really have a intelligent, or even a half way educated conversation about this technology.

[0:09:07.5] JM: Yeah. How do you allocate your time between studying cryptocurrencies, versus other classes? Are there classes at Waterloo now where they are teaching the stuff?

[0:09:17.2] SN: No. At Waterloo there is, as far as I know no such focus on blockchain technologies. I remember reading a little bit. Some colleges are introducing courses in cryptocurrency, which is pretty cool to see. For me personally, the reason why blockchain is intriguing is first, there is this whole entrepreneur side of it. There are companies popping up left and right trying to incorporate blockchain into anything that they can get their hands on, any company they can get their hands on.

MongoDB has come out with their own enterprise blockchain for example, which is insane and I have no idea how that works. That's just one example of how all of this is revving up in the entrepreneur world. That's where my interest stems from, this entrepreneur side of things. Back in the summer, I saw all these companies popping up. I was like, "Yeah, I got to hop onto this bandwagon." Because I like coming over these ideas and the potentials to our business is very appealing to me even as a student.

Then I took a step back and I realized, "Hey, it would be a lot better for me to understand how this technology works as an engineer, because then I can work on building these solutions and working on top of these solutions in the future by having a fundamental understanding of it."

For me, really it's just prioritizing what I want out of my career in the future and that's really to build a solution and have a fundamental understanding of a solution that can disrupt something – meaningful way, in a meaningful manner. That's where this interest of taking a step back, looking at the fundamentals, looking at how the technical details of blockchain technology work. Anybody out there, I think should do the same if they're really, really interested in delving into this technology.

[0:10:51.1] JM: Well, in contrast to the approach of trying to start a business today or perhaps trying to mold some semblance of a business solution into something that could ICO. I think the education approach is just much safer, because in the universe where these ICOs, or these short-term businesses end up not blowing up, or ending in jail time or SEC fines, or getting hunted down by your token holders, in the universe where those do not end up in catastrophe,

that is some universe where cryptocurrencies and decentralized technology has really taken hold in a meaningful way as opposed to a thought experimental way, which to be clear we're pretty much still in the thought experiment phase.

If that universe holds true, then your investment in knowledge will probably lead you to opportunities that are going to be at least as financially profitable as the short-term ICO, short-term business that you might have started today would have been. You're probably not even giving up anything by not – even not investing in cryptocurrencies themselves, even not buying Bitcoin and Ethereum and instead spending your money on Udemy courses or something, or like a gym membership is probably more worthwhile.

[0:12:30.4] SN: Absolutely. That's actually another big reason why I believe education in this field is a lot more fundamental than just bypassing that and trying to dive in and get your hands on an ICO or stunt building a token. I'm skeptic when it comes to this field and I feel like everybody should be a skeptic, because like you said, we're in a very thought experimental phase when it comes to this field.

There's a lot going out there that I don't understand, a lot of people don't understand. Frankly, every day there's something new that just keeps popping up that really – nobody really understands, but everybody is trying to monetize and capitalize upon. That's something that has to be looked up very, very carefully in this field.

If you make an effort to really understand how this technology works, how it can be applied, the pros and cons of every single project that you may potentially want to look at, invest in, or build, if you could do that in an educated manner, then like you said, you have a far better chance of being profitable, of making an impact, of not ending up in handcuffs down the road. That's really, really one of the most important things to realize in this field.

If you don't really understand what's going on here, it's a very dangerous thing to get into, because you could very easily get caught out of your money, build something that makes other people lose their money, or just break the law, break regulations upon you that you didn't intend and consequences that really won't be great for you.

That's why every single – I have a lot of colleagues that approach and they told me about new projects coming out. Every single one, I take a skeptical approach to it and I take a very educated approach to it. Even Bitcoin itself, when everything started to click for me six or seven months ago when it came to understanding the technology, I was skeptic. I took my time, I understood the realized impact of this technology. Then from there, I started to teach about it. [SPONSOR MESSAGE]

[0:14:32.0] JM: QCon.ai is a software conference for full-stack developers looking to uncover the real-world patterns, practices and use cases for applying artificial intelligence and machine learning in engineering. Come to QCon.ai in

Come to QCon.ai in San Francisco from April 9th to 11th, 2018 and see talks from companies like Instacart, Uber, Coinbase and Stripe. These companies have built and deployed state of the art machine learning models, and they've come to QCon to share their developments.

The keynote of QCon.ai is Matt Ranney, a Senior Staff Engineer at Uber ATG, which is the autonomous driving unit at Uber. He's an amazing speaker. He was on SE Daily in the past. If you want to preview for what he is like, then you can check out that episode that I did in conversation with him.

I've been to QCon three times myself and it's a fantastic conference. What I love about QCon is the high bar for quality, quality in terms of speakers, content and peer sharing, as well as the food and the general atmosphere. QCon is one of my favorite conferences. If you haven't been to a QCon before, make QCon.ai your first.

Register at qcon.ai and use promo code SE DAILY for $100 off your ticket. That's qcon.ai and you can use promo code SE DAILY for a $100 off. Thanks to QCon for being a sponsor of SE Daily. Check out Qcon.ai to see a fantastic cutting-edge conference.

[INTERVIEW CONTINUED]

[0:16:18.0] JM: It's funny, because even the people who are teaching Bitcoin, like I just interviewed Joseph Bonneau a few days ago and he was one of the instructors for that really

good series of video that Princeton put out about cryptocurrencies and he's one of the co-authors of that textbook that came out that was really good, but a really good textbook on Bitcoin.

He's skeptical that Bitcoin will even be here in five or 10 years. Here is a guy who is definitely in the top 0.1% of people in the world who understand these things and has essentially given his entire intellectual horse power towards understanding and he's skeptical of the godfather of cryptocurrencies. He's skeptical of Bitcoin. If there is a sign that this stuff is important from an intellectual pursuit and perhaps maybe not from a present day financial market use case implementation pursuit, I mean I take that as a pretty strong sign.

That said, I mean you must have. I know how students think and I know how the minds of students can work at a frenetic pace, such that something like day trading cryptocurrencies is actually something that a student – they have the mind to do it, that 17-year-old, 18-year-old mind. I know this because I used to play poker and your mind is attuned to being really good at things like video games and things that can just have a feel for the market, or a feel for the game.

It's like the prime of your age – given that you go to Waterloo, you must be around some pretty sharp kids that are day trading and they must be making millions. Are you having to quell some fomo when you're talking to the day trader types?

[0:18:12.1] SN: Yeah, absolutely, absolutely. At my office, I work for a startup in Toronto called Fix. The average age here is I think 24, 25. Everybody is nuts for cryptocurrency. Conversations are happening daily, all of my friends are having conversations about cryptocurrency. You head over to Waterloo, there is hackathons happening, based your own Ethereum.

For anybody who knows CryptoKitties, the most popular Ethereum application in the world, it came out of Waterloo in a 36-hour hackathon. All this is happening at an incredibly rapid pace all around me. You're right, you feel that fomo, especially when it comes to investing your money, you feel I want to dive into this, everybody around me is making millions, I personally know a few people who have definitely made an insane amount of money that I wouldn't not have been able to realize.

I take that feeling and I – again, I invest it into education. I personally – I do not like speculating on the price of any cryptocurrency assets, just because of the inherent volatility that exists now and it will probably exist for the near future and the far future. Whenever somebody asks me, "What do you think of this cryptocurrency? Should I invest?" I tell them to instead look at the education. Learn something about it. Educate others about it.

There's a lot more inherent value in that and that will make you be able to understand this technology at a much better level in the future. At that point, you can make that decision for yourself. Is this technology valuable enough to make an impact? What are the cons of this technology? Will this technology ever go to zero, could ever go to zero? I know this because I've research the technology behind it.

At that point, I feel like you don't need to ask anybody. You can make that decision for yourself. That's really where I stand when it comes to all of these hype and buzz around me. I much rather try creating something of my own, or researching the technology at another level, rather than try to invest in something at this stage of the cryptocurrency, like market at least.

[0:20:08.7] JM: Before the show, we were talking a bit about your article that you're writing right now, which is about proof of work versus proof of stake and some aspects of Bitcoin mining. I'd like to dive into technological discussion with you. In order to warm people up for a proof of work versus proof of stake conversation, I believe most of the audience is at this point if they're tuning in to this episode, they probably at least reasonably familiar with how transactions are processed in Bitcoin. Maybe you could just give people a little bit of a stretching exercise, warm us with how are transactions processed in Bitcoin.

[0:20:48.2] SN: Absolutely. I own a Bitcoin, I want to send it to Jeff. What I do is I take my Bitcoin wallet and I send it to my nearest node, or a node that I trust. I say, "Take my 1 Bitcoin and give it to Jeff." This nodes propagates it all across the world until it gets to a miner and actually all miners will receive this transaction that I'm willing to execute.

Once a mining node or a miner receives this transaction, what they do is they conduct an algorithm called proof of work. With proof of work, it is essentially a state of a massive amount

of electricity and time in order to verify that this transaction is in fact valid. It's what it is is at a very high level it's a cryptographic puzzle. Once they solve this cryptographic puzzle, they publish this verified and cryptographically solved block, which consists of my transaction and many others to the rest of the network.

The rest of the network accepts this transaction is true and they start building the next block upon it. That is essentially how the blockchain network operates and validates transactions. I hope that's a good high-level explanation to everybody out there.

[0:21:59.5] JM: That's great. Just to put a few more points on that that might be relevant to our conversation. If you're going to transfer Bitcoin to me, you are issuing a transaction. That transaction is I'm sending 1 Bitcoin to Jeff and that's the data load that you're going to send to any Bitcoin full node in the network. That transaction goes into that node's mem pool, which is the in-memory set of transactions that have not been accepted by the network yet.

Periodically, a Bitcoin full node is going to pull a set of transactions from that mem pool into a block and they're going to start to try to calculate the solution to a puzzle that turns that block into an acceptable set of transactions for the Bitcoin network. If they successfully solve that cryptographic puzzle, then that means that they have proved that this block is acceptable to the network and they will publish that block and its solution to the other full nodes, so that the other full nodes can see, "Hey, somebody has a new block," which means that they have a longer chain of blocks than anybody else in the network.

We need to accept this so that we can start working on a fresh set of transactions to include in a new block, so that we can win the prize that's associated with the next block of transactions. There can be some churn in there. If two people solve disjoint puzzles at the same time, then you can have different blocks that get calculated and get accepted to the blockchain, which means that if I'm trying to verify that I got a Bitcoin from Subhan, then I may want to wait for two or three blocks, or six blocks or however many blocks I need to feel comfortable before I say, "Okay, this transaction has been fully accepted by the network. It is very likely to be undone, or to be double-spent." Is that accurate information?

[0:24:10.3] SN: Absolutely. A lot more detail than what I just said. Yeah, absolutely accurate. Just a quick distinction that I want to make, so you mentioned that there are full nodes that pull

the transactions out of the mem pool and then attempt to calculate this proof of work algorithm in order to publish the block.

What happens is that the majority of nodes that exist today are actually full non-mining nodes. What these nodes do is they conduct economic transactions and they propagate blocks or transactions across the network.

You're right in the sense that each node has a mem pool. This mem pool holds almost every transaction out there. Say for transactions that have too low of a fee to be accepted. Then these full non-mining nodes propagate the block, or propagate these transactions to mining nodes that then pull them out of their own mem pool and then start mining.

[0:24:58.3] JM: Okay. That's a good point. That said, what do people misunderstand about Bitcoin mining most frequently?

[0:25:06.3] SN: I think the biggest misunderstanding is its security. A lot of times, because it is a very fundamental, it is a little bit of a choky concept to grasp, people underestimate the security of the network. At a very high-level, or in very basic conversation, to this day you still hope people would say Bitcoin's insecure, it's a scam, etc., etc.

That's because the fundamental value of proof of work isn't realized. The fact that this algorithm has been able to secure the network and thousands and hundreds of thousands of transactions over 10 years is entirely ignored, because the value of proof of work is not fully realized and fully understood. That's really where a lot of misunderstanding comes.

Not so much these days if you're into the blockchain technology field, everybody has realized, a lot of people have realized within the cryptocurrency field itself that proof of work is proven to be a reliable fault tolerant system when it comes to securing the blockchain. Outside of that community, there is still is a lot of misunderstanding and a lot of educating that needs to be done about the security of it.

[0:26:12.5] JM: Just to give a little bit more color on the basics, explain the interaction between light clients, like a wallet, like a Bitcoin wallet that I have on my phone. What's the interaction between a light client and a full node?

[0:26:27.4] SN: Absolutely. What a full node does is it communicates with other Bitcoin fully nodes and upon a fresh start, it downloads every single Bitcoin transaction on the blockchain from the very first day, downloads it from these other nodes and then it begins to validate every transactions starting from day zero. Builds its way up the blockchain, begins to validate the transactions, the inputs and outputs to each transaction, all the way until we get to the current and most recent block.

I believe currently, the blockchain is about a 150 gigabytes in size, so it will download all of that, start validating every single transaction until it gets to the most recent block. Then that full node is responsible for propagating new transactions and validating new blocks that it receives. A full node is as you can imagine a very intensive computer per se. It needs a fair bit of storage, a fair bit of bandwidth because it's propagating transactions an blocks to several other nodes on a 24-hour basis. As while it requires a larger amount of storage for the blockchain itself.

Full nodes are not what you and I would use on a daily basis to transact with Bitcoin. You and I would use something called the light wallet, like you said. What the light wallet does is it downloads a summary of each block from the blockchain called the block header. The block header is a easily verifiable hashed summary of each Bitcoin block.

It's only 80 kilobytes approximately per block. What my light node can do is it can query my nearest full node, ask for that block header, or for all of those block headers, verify that this chain is valid by hashing each block header and upon doing so, it can then propagate new transactions to full nodes, which then send it around the network. Light nodes essentially act as user-friendly clients, or they're called SPV clients technically. They're really built for data to use for Bitcoin.

[0:28:30.0] JM: Not to get too technical here, but I've been trying to figure out what is the best way to explain the importance of the Merkel tree in the interaction between light clients and full nodes. I've been trying to basically indicate to the listeners that the Merkel tree is a data

structure that is worth inspecting without trying to explain what Merkel tree is on the show, because I think it's hard to explain.

[0:28:54.6] SN: Absolutely. Yeah.

[0:28:55.9] JM: I would just say for anybody that's interested in data structures, it is one of the coolest data structures, I think I still don't have a good enough understanding of it to explain it and perhaps even to grasp the importance of it. Maybe you could explain at least why is the Merkel tree such an important data structure. Why is it essentially key to how the Bitcoin network works and how it's actually usable?

[0:29:23.5] SN: The way I like to describe a Merkel tree is that it's a summary. It's a verifiable summary of all the transactions, or all of its children that exist. Currently, Bitcoin transactions are stored in a Merkel tree. The root of this Merkel tree stores – is essentially a summary of every transaction that exist below it. Without having to download every single transaction making sure that every single transaction is valid, as long as other nodes have accepted the root of a Merkel as valid, all you – this root of the Merkel tree is just a few bytes long, all you have to do to ensure that the transactions for any particular blockchain is valid is to just look at the root of the Merkel tree, compare it to other nodes, roots of the Merkel tree and make sure that is valid.

The reason why it's so important is because no matter how many transactions, you could have thousands or hundreds of thousands, millions of transactions within a tree. No matter how many transactions you have, all you really have to do is look at the root of this tree to say, "Hey, all these transactions still exist within this tree. This I believe maybe 10 kilobyte long root verifies that these transactions exist, and so that's all I have to worry about. I'll download this block, accept it as valid. We're good to go." No issues in terms of validating every transaction from the bottom up. It really is just a verifiable summary of transactions that exist on the blockchain network.

[0:30:51.9] JM: It's compact, so that even if I'm running a light client on my phone that has the Merkel tree, that's all I need in order to verify that a certain transaction that – if I've got a light client and my light client is in a relationship with a full node and it's using that full node as the source of truth and it's like pinging that full node, or maybe it's pinging a couple full nodes and

saying, “Hey, what’s the state of the blockchain? Just give the digest, give me the block headers and I’ll build my Merkel tree out of them and I can verify whether transactions are legitimate or not, even though I do not have an entire full node myself.” Did I get it right?

[0:31:37.8] SN: Yeah. Essentially, all you really need is – what a full node will do is they’ll accept the entire set of transactions in a new block and they’ll go to every single transaction and they’ll say, “Hey, this transaction is valid because Subhan previously did own a Bitcoin. He’s sending it to Jeff and also Jeff has a Bitcoin.”

It’s a little bit of a caveat, but it’s interesting, because every transaction in a Bitcoin on the Bitcoin network is essentially routing Bitcoins from one address to another. Nobody really owns Bitcoin. Bitcoin, what happens is when a miner successfully creates a block, they receive a certain set of Bitcoin. That’s when Bitcoin is created. Then every single transaction for those Bitcoins is validated by just simply looking at where that miner sent the Bitcoins to. For example, we have a miner send that Bitcoin from point A to point B, they will validate that. Then that same Bitcoin will be sent from point B to point C, and it will validate that.

All we’re really validating is the route that the Bitcoin took to get up to the latest block. What this Merkel tree, what this full node would do is it will validate this route. It will say, this Bitcoin has successfully come from the miner through all these people, to this person. I accept that and it’s a part of my immutable blockchain ledger. The full node will keep it, and so the Merkel root of the tree that miner holds for all the transactions will be this few kilobyte long string that is immutable, that will always exist and that will always represent the transactions that full node is accepting.

Now if I as a wallet want to see if that blockchain – if that block header and those transactions are valid, all I have to do is I’ll have to download the block header, I’ll have to hash it and then I have to see if the hash matches what the full node propagates. The hash will include the root of the Merkel tree, so the Merkel tree is bundled up into the block header.

As long as the hash is the same as what the full node has propagated, we’re good to go. All I have to do is conduct a single shot 256 hash function, see if the output matches with the full node, is outputting and then we’re good to go. As a light wallet, I really don’t even need to

download any transactions within that block itself. I just have to look at the Merkel root and then the block header itself, which is only 80 kilobytes large.

[0:33:57.2] JM: All right. We have properly set the table at this point. Let's talk about proof of work and proof of stake. The system that we've described is proof of work; miners validate transactions by solving cryptographic puzzles associated with a set of transactions. Those set of transactions turn into blocks that are verified.

Proof of stake is quite different. It replaces this system, which is energy-intensive, because these miners are doing these repeated calculations to attempt to solve cryptographic puzzles. By the way, they're all doing similar cryptographic calculations in parallel and only one of them is going to solve a block, so there is a whole lot of wasted work that's essentially going on.
I mean, it's not actually wasted because we don't know a better way of doing this. Maybe proof of stake is a better way of doing this, but we know that proof of work works even though it takes a ton of energy. It's just the only way that we know works right now that at least has been implemented. Proof of stake is different. Explain what proof of stake is.

[0:35:05.9] SN: Absolutely. Again, at a very high-level, proof of stake is essentially a group of individuals who have an amount of cryptocurrency, so for example they have some level of Ethereum in their possession. What they do is the stake datathereum onto the blockchain and then say here is X number of Ethereum, block this up in the blockchain, I'm not allowed to use it. What this Ethereum represents is my ability to have a vote on the validation of a block.

What the network will do is it will look at everybody who staked some level of their cryptocurrency and they'll say deterministically and using a probability function, what it will do is it will select an individual who has staked their cryptocurrency. It will hand them the blocks on the network, or the transactions on a network waiting to be confirmed and it will say, "Here, validate this block. Just do it." We'll wait for that person to validate the block and this person will then propagate this block to others once it has been validated.

The reason why this is considered to be secure is that this individual has staked some considerable amount of their own cryptocurrency. In doing so, they're essentially trusted to validate this block in a way that other nodes will accept this truthful. If they fail to validate this

block in a way the other nodes accept to be as truthful and instead they do so maliciously, the cryptocurrency that they have staked is lost.

All other truthful nodes will essentially deem this malicious actor as actors block as invalid and it will deem their cryptocurrency that they have staked as gone. It will vanish. They are out of whatever they stake. What the system does is introduces a completely new paradigm when it comes to potentially validating and securing the blockchain.

[SPONSOR MESSAGE]

[0:37:04.3] JM: Software Engineering Daily is brought to you by ConsenSys. Do you think blockchain technology is only used for cryptocurrency? Think again. ConsenSys develops tools and infrastructure to enable a decentralized future built on Ethereum, the most advanced blockchain development platform.

ConsenSys has hundreds of web3 developers that are building decentralized applications, focusing on world-changing ideas like creating a system for self-sovereign identity, managing supply chains, developing a more efficient electricity provider and much more.

Listeners, why continue to build the internet of today when you can build the internet of the future on the blockchain? ConsenSys is actively hiring talented software developers to help build the decentralized web.

Learn more about consensus projects and open source jobs at consensys.net/sedaily. That's C-O-N-S-E-N-S-Y-S.net/sedaily. Consensys.net/sedaily. Thanks again, ConsenSys.

[INTERVIEW CONTINUED]

[0:38:20.6] JM: If you think about Twitter. On Twitter, the people who have a blue check mark next to their name, they have been "verified." Whatever that means, they have been verified. In some sense, that's similar to the fact to the idea of proof of stake, because these people have gotten verified because they have either a public identity that is important elsewhere and they're not going to taint that public identity by publishing false, or cruel information on Twitter.

Perhaps, they've been on Twitter for so long, they have a massive following and they've got a bunch of fake accounts that are trying to impersonate them. They've got a blue check mark and they're going to be unlikely to do something that would make them an unverified user, because if they lost that blue check mark they would be subject to all kinds of masquerading attacks and so on.

The idea is that the people who received the blue check mark on Twitter are generally people who have an incentive to maintain and in fact improve the quality or the worth of that blue check mark. It will be a self-regulating system, because sometimes people who have a blue check mark and engage in malicious behavior, they have a bigger spotlight on them so they kicked off a network more aggressive, or they can lose their blue check mark I believe under some circumstances.
Similarly, in proof of stake you've got this pool of validators who have been chosen by the network as validators who are – the network is important to them, so they have a stake in the network. They've got a lot of Bitcoin, or they've just been validating transactions for a long time perhaps. I would love to get into how validators are chosen.

Not only that, if they do something wrong, if they try to validate – if they are chosen by the network to validate a set of transactions as being valid or invalid. There is an invalid transaction and they make a mistake, then if the network detects that later on that they've made a mistake, the network is going to subtract all of the Bitcoin that they own so that the stakes are pretty high to be truthful in your validation. Is that an accurate picture I have painted?

[0:40:35.3] SN: Absolutely. Yeah. The Twitter analogy is actually a very good one. The only thing I would say about that is I don't know how much value people would see on having that blue check mark. I'm sure many individuals would, but at the same many individuals have happened to lose that check mark. I don't know how much of an impact they would have on them.

However, with proof of stake, what you're staking is your money, you're staking savings. You're staking something that has quite literally a financial impact. There is a lot more incentive for you to do very little wrongdoing here. Yeah, everything else you've said is quite correct. You stake

cryptocurrency. Bitcoin in my opinion, I don't see it moving to proof of stake anytime soon, but Ethereum for example would be a good example would stake Ethereum.

They stake their Ethereum and proportional to their stake, a probability is assigned to them being chosen to validate the next block. It would be in their very best interest to validate it correctly exactly.

[0:41:29.5] JM: How do people end up in the validator pool, who can be randomly selected to validate these transactions?

[0:41:36.6] SN: All you really have to do is stake some level of Ethereum. Right now, the biggest proof of stake counts a prototype and test of concept is happening on the Ethereum network. It's not has been published there yet, but it is being tested. Ethereum will most likely move to a proof of stake system within the near future.
All an individual really has to do is conduct a transaction saying, "I have X amount of Ethereum. Lock this up and consider me a validator." As long as they had that Ethereum, they will be in a very decentralized and trustless aspect, they will be considered as a part of the validating pool, as a potential person to be selected.

The most cryptocurrencies you stake, the higher probability you have of being selected. This is because you have a higher stake to lose, why not give you a chance and see if you can validate it properly.

[0:42:30.8] JM: The important part of this is that if you validate a transaction that we later find out is incorrect, two things need to happen; first of all, we need to take all your cryptocurrency that you've staked and grab it from you. Two, we also need to roll back the blockchain somehow and undo that transaction. What is the process of validating the validators?

[0:42:53.7] SN: That's a good question. I'm not too familiar with the intricacies of proof of stake itself when it comes to rolling back and handling – punishing validators. That's something I will be researching in the future. Right now, I'm focusing a little bit more on proof of work.

[0:43:06.6] JM: We'll be doing several more shows on this topic. I think I already have a show about Casper scheduled, so I'm sure we can go a little bit deeper in that episode.

[0:43:13.7] SN: Absolutely, yeah. I'm actually in the process of reading the Casper whitepaper right now, which is why I'm not entirely versed in how punishing a validators happen.

[0:43:22.7] JM: Totally fine. What's that experience been like? By the way, how do you attack these whitepapers? Some of these are pretty dense?

[0:43:28.3] SN: They are. They are. Time, honestly all you really need is time. Again, starting from a very fundamental level really helps. For example, I tried diving into how Ethereum worked before how I learned how Bitcoin worked. Did not happen. I went back to square one, I read the Bitcoin whitepaper. There's an incredible amount of resources out there that are based around learning Bitcoin. I read a fair amount of them.

That's where I really started to feel confident about being able to learn other concepts, such as how the Ethereum network works, concepts such as how the lightning networks works and again, concepts such as proof of work and how Casper will be working in the future. Again, just starting from the fundamentals and working your way up from there will save you time down the road when you try to get into more complex topics in the field.

[0:44:16.1] JM: It's so true. I'm laughing because I think it was the second or third week of shows on Software Engineering Daily that I did shows on Bitcoin and Ethereum, mind you, without really understanding how the stuff works. It was just a train wreck. I try to do a show on lightning networks and I had some good questions to ask, but mostly I had no idea what the questions I was asking meant. I just knew that they were questions that other people were asking, which is just not a recipe for walking away with a good understanding. Yes, I think we rehashed this several times in the introductory questions, but always better to start with the fundamentals.

[0:44:54.4] SN: Absolutely. Yeah.

[0:44:56.3] JM: A little bit more about proof of stake. In some sense, this leads to a rich get richer problem, because the people who have the money to stake can earn interest on that money. Is this a rich get richer problem? Is that leading to further centralization? Is that problematic?

[0:45:17.8] SN: Absolutely, yeah. That's something I've definitely been considering and looking into. Proof of stake works to solve a lot of the issues that proof of work has. The expenditure of an insane amount of electricity, the potential centralization risk, making the 51% attack a little harder, because there's no mining at work. All you're really doing is randomly selecting people to validate the network.

You're right. There is this risk of the rich get richer potentially when it comes to proof of stake. The argument could be made that those who stake a large portion of their wealth in order to secure the network deserve to make that money, deserve to reap the benefits of it. That same argument has been made about the small number of wallets that hold large number of Bitcoin.

Maybe the early adopters of Bitcoin deserve to hold and reap the majority of the benefits on the network because they took such a massive risk early on. I personally wouldn't agree with that mentality, because again, the point of decentralization, trustlesness and sensor-resistant premises is to put the damper on corruption, to reduce the level of corruption and centralization and the corruption and the abuse of power that comes from centralization.

Although that argument that can be made, the fact that people who take a greater risk early on, or stake a lot of the currency should reap benefits down the road, there is always a possibility that power and a large amount of control over any system will corrupt any individual. That may and that will probably will happen if centralization again becomes a theme in cryptocurrencies. Yeah, that is a very real risk when it comes to proof of stake in my opinion.

Again, I have to do a lot more research on this field and see perhaps if there is a way to tackle this. Yes, the rich getting richer is a problem. However, it is important to note that when you're considering the probability of somebody staking 10,000 Ethereum versus 8,000 Ethereum versus 7,000 Ethereum versus 5,000 Ethereum, you're probably going to have a relatively negligible risk of the rich get richer/centralization problem.

When you consider the extremes of this, what a lot of people think is the probability of somebody staking 10 Ethereum versus 1 Ethereum. The persons taking 10 Ethereum is definitely going to have a much high probability being selected and then a much higher probability of earning more Ethereum, and so the rich get richer.

When you consider a fleshed out – a relatively fleshed out system like Ethereum, you have a lot more decentralization, a lot more distribution of the current currency and there will be a lot more competition when it comes to staking their currency's proof of work.

There is definitely a real probability of the rich get richer problem being negligible, but that again remains to be seen. For me myself personally research has to be conducted before I can make a definitive conclusion about that.

[0:48:17.8] JM: The other aspect of that is like if you want to stake so much Ethereum, or so much ether that you're just going to dominate in the rate of being selected to validate blocks, you're probably going to be staking so much ether that your funds would be better sent elsewhere. It would just make more sense for you to allocate them into index funds, or something else, because this is essentially like a bond, like an interest-bearing instrument with a pretty predictable interest rate.

If you just say, "I want to dominate and always get that small amount of interest, you might have to make a very irrational bet if you really wanted to dominate it that bad." It doesn't have the same problem of being subject to a 51% attack, because anybody can always check your work. If they prove that you're doing something wrong, then you just lose all of that money and it's just like – it seems like a very sensible solution to me.

[0:49:18.1] SN: Yeah. Yeah, what you mentioned is actually a valid point and it's actually a fundamental aspect of the game theory that exist not just behind proof of stake, but as well as proof of work. If you look 51% of tax in Bitcoin, if you're a miner and you have 50% of the hashing power in the network, it would probably still be in your best interest to keep mining and not double spend your coins if you happen to have the majority of hash power, because if you

do that, you will get caught and you will propagated off the network. You will not be able to make any more money profits.

That's a very valid point, that a lot of people will act rationally. Again, with proof of stake, the exact same mentality comes to play. If you have 30% or 40% of the network stake using your own currency, it would probably be in your best interest to act truthfully to better your holdings.

[0:50:11.8] JM: The other issue at hand and this is somewhat tangential is that one of the problems of proof of work is proof of work leads to hardware centralization in a very physical manifestation, which is problematic. Okay, proof of work functions today, like that's great. What happens when government currencies start to not look so appealing for any use case?

That is a potential outcome. When that happens, if there is a hardware centralization, that's a centralization that is existent in the physical world and governments are pretty good at administering control over physical assets and disrupting physical assets. Proof of stake in contrast seems like a more ephemeral consensus mechanism that would not be centralized in any particular hardware dimension.

[0:51:06.7] SN: Absolutely. The technical beautify of proof of work is that if you happen to restrict for examples the sales basic mining hardware, which is what's used for the majority of Bitcoin mining today, the difficulty of the network will go down and [inaudible 0:51:20.3] will be able to mine Bitcoin let's say at a very extreme level where the GPU is again.

That level of technical decentralization and the level of access would still be available to individuals, despite the restriction of hardware. The difficulty of Bitcoin scales with the level of has power that the network has. The reason why proof of work is determined to be effectively secure; if somebody wanted to launch a 51% attack on the Bitcoin network, they would have to spend I think awards of millions or potentially even billions of dollars and they need to purchase enough hardware and expend enough electricity to make that happen.

That's really where proof of work is expected to be relatively secure, despite the fact that like you said, there is dependency on hardware and hardware can be restricted. The difficulty with

adjustments that happen on the Bitcoin network both stem to prevent an extreme level of attack by the government, or otherwise.

Again, like you said, there is an inherent disadvantage through relying on hardware. That is potential restrictions in the short-term that may happen and as well as the over-looming environmental impact that comes from such expanded hardware usage. Proof of stake is valuable in that sense.

At the moment, this rich get richer problem and as well as the fact that nobody has really been able to successful implement it and ensure that it's attack resistant is a very important aspect that you're going to be neglected. The reason why Bitcoin can be deemed as secure is because it has existed for 10 years with proof of work, and like you said it works and it hasn't been – the network has not been able to be attacked and that's proved it.

You put something out there and you let it be attacked. If you can see that is resistant, there is some great inherent value with that. Hopefully proof of stake gets to that point, we can say, yeah proof of stake works. It's a better alternative. Until then, it's a very fine line to tether across when trying to talk about the long-term effect of nature of proof of stake.

[0:53:24.1] JM: One thing I think that is ironic about these systems, like we call it proof of work or proof of stake. They're proof-based systems, like you can prove that you have done the work to validate some transactions by presenting the solution to a cryptographic puzzle. You can similarly prove that you have a stake in the network by giving some ether. What I think is funny is that the only way that we know that these systems work is if we actually deploy them and then test them and have empirical data to show that they work over time and that nobody has found a vulnerability in them, which is not at all what a proof is in fundamental computer science terms. I just find it hilarious.

[0:54:10.9] SN: Yeah. That's honestly when Bitcoin, if you'd go all the way back to 2009 and you look at Satoshi Nakamoto's old e-mail lists. He was skeptic. He was like, "Hey, I don't really know if this is going to work. Just try it out." People just started throwing things at it, people built on it. Nobody really knew if it was going to be secure or if it worked.

Attacks happen. They were attempted. It continue to resist and become resilient. It's essentially evolved into what we have today, which is something that we know is works. Like you said, it is – if you think about it, it's ridiculous. How can you expect the system to be secure when you just let it live and you see what happens to it?

I agree with that, absolutely. That's really why when you look at something like Bitcoin for example, I can't question its immutability and its security, because all that has happened and we're at this point today where nothing has changed about it. We can effectively trust that the system works.

[0:55:11.9] JM: Although, equally hilarious when you talk to economic traditionalists and they are just looking for an excuse to dismiss cryptocurrencies. They hear about the deflationary argument. "Oh, Bitcoin is deflationary." We've seen what happens with deflationary currencies. People just don't spend them. Therefore, because people don't spend them and we know that they just increase in value over time, this will not work as a currency, therefore I can ignore this space entirely and dismiss everything else that you're saying to me.

When in fact, the only – as far as I know from these conversations, maybe there are more data points on this, but the main data point has something to do with Japan, like Japan had a deflationary currency for a while and that was catastrophic. Maybe there are some other examples, but I don't know. Maybe I'm talking with a little too much conviction here, but it just seems like we just don't have much data in terms of testing different economic systems.

We just really don't have a whole lot of data. Anybody that says, "Oh, we really know this. We are so sure of this thing about economic systems." Talk about skepticism. I'm pretty skeptical of people who are so economically sure of something like that.

[0:56:25.5] SN: Absolutely. Again, people who are skeptical of the impact of Bitcoin potentially being deflationary, I give them credit, you should be skeptical. Should you dismiss Bitcoin, its technology and its impact because you're absolutely sure that it will cost a deflation spiral and destroy the economy? I'm sure well on the same page, I disagree with that kind of mentality.

There is something to be considered when it comes to Bitcoin. It has a limited supply, it's immutable and it's inflation right now is controlled every sense of the way. There's value in that but at the same time there are economic impacts that remain to be seen when it comes to widespread adoption of Bitcoin.

We don't have enough data. You're right. We will see what happens. I personally don't feel like any level of adoption of Bitcoin would be a bad thing for the economy. I personally feel like inflationary currencies will continue to exist, but there is something to be said about Bitcoin being used as an inherent store value that will continue to grow and be immutable in the future.

[0:57:26.9] JM: Right. Yeah, maybe a deflationary store value is great. Maybe it's not so useful as a currency.

[0:57:31.9] SN: Absolutely. You're right. Again, everybody should be doing their own research about the economic impacts of Bitcoin itself. For me, that's also one of the great appeals of Bitcoin. I'm studying business as well and I'm taking a minor in economics. This is a very basic economic concept, deflationary spirals versus the impact of inflationary economic incentives.

Seeing how Bitcoin not only has impacted the wealth of technology, but as well as an impact in the world of economics and the way we use currencies and grow our economies itself is something that's very, very, very intriguing.

If you are interested in seeing how the world may change because of this technology, the economic aspect of Bitcoin should absolutely be studied rigorously. That's something I've been doing and I hope to do in the future as well.

[0:58:22.2] JM: Let me ask you another technical question about proof of stake. Does proof of stake improve scalability? I understand that it alleviates the electricity demands, but I imagine if you can have this network where you've got these validators and you can just say, "Okay, we've got this pool of transactions." We can actually do things in parallel now, because we can just take different sets of validators and throw disjoint sets of transactions at them, and we can get a whole lot more transactions validated in the same amount of time, rather than redundant proof of work systems. Is that accurate? Is proof of stake more scalable? Does it add to scalability?

[0:59:03.9] SN: Absolutely, yeah. That's actually a very interesting topic to consider. The reason why a lot of the restrictions exist in the Bitcoin network are because of the proof of work algorithm. For example, currently the block size is approximately 1 megabytes, would segway it up to 4, relatively small. One of the reasons why that is is because miners are expected to mine a block within 10 minutes.

Then this new block that they mine is expected to be propagated across the network, as soon as they mine it and it's expected to propagate relatively quickly, because miners didn't have to spend up to 10 minutes mining the next block. A considerable level of time is expected to be expended mining every single block.

Proof of stake, what that effectively does is it eliminates that kind of time constraint. It eliminates that expected expenditure of time and very hypothetical terms. The validation of a block is almost instant. What that means and the implications that it has is that you're able to propagate blocks at a much faster level and while potentially reducing the level of orphan chains. What that means is that chains that get left behind, because the blocks got propagated too quickly.

You're right, if the validation of a block is almost instant, then blocks can potentially hold many more transactions, a lot more protocol changes that can come into play, because block propagation and block time restrictions are not as big a part of the equation anymore.

[1:00:40.0] JM: All right. Subhan, it's really been great talking to you. I could continue talking to you for a long time, but I know we're up against time. Yeah, I guess well, one of the question, so you're looking at computer science and business at the same time. I know you're not going to start a business anytime soon probably, or maybe you are thinking about it. You got some ideas?

[1:01:00.0] SN: Yeah. Well, I have some inspiration. I'm working for a company called Fix in Toronto right now. The CPOs 23, the CTOs 24 and the COs 27. These guys are tempting to start a business. You never know. Could happen. Yeah, go ahead.

[1:01:16.5] JM: You got any ideas yet, or nothing you can talk about publicly?

[1:01:19.1] SN: Yeah, nothing I really want to delve into yet, but we'll see.

[1:01:22.3] JM: Okay. All right. Well, we can do another show in the future.

[1:01:24.7] SN: Absolutely.

[1:01:25.5] JM: Subhan, thanks for coming on Software Engineering Daily. It's been great talking to you.

[1:01:28.0] SN: Absolutely. Great talking to you as well, Jeff. Thank you very much for everything.

[END OF INTERVIEW]

[1:01:34.0] JM: If you are building a product for software engineers, or you are hiring software engineers, Software Engineering Daily is accepting sponsorships for 2018. Send me an e-mail jeff@softwareengineeringdaily.com if you're interested.

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

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

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

[END]

