EPISODE 449

[INTERVIEW]

[0:00:13.9] Host: Vlad Zamfir is a researcher for the Ethereum Foundation. He is a mathematician and statistician by hobby, you can maybe clarify, and is the chief researcher behind Casper, Ethereum's new proof of stake-based consensus protocol. He's an active blogger and speaker and writes a lot about the field of cryptoeconomics.

Vlad, welcome to Software Engineering Daily.

[0:00:31.9] VZ: Hi, Z. Thanks for having me.

[0:00:33.9] Host: Yeah, of course. I'm really excited to talk to you actually. One new area of research development in the world of blockchains is what's called cryptoeconomics. Cryptoeconomics is sometimes described as the intersection of distributed systems, economics, game theory and cryptography. Let me start by asking you, how would you define cryptoeconomics?

[0:00:53.5] VZ: Sure. Yeah. From my point of view, cryptoeconomics is the application of incentive design to problem that are traditionally cryptography and distributed systems problems. Basically, there is like a certain type of problems that like crypto industry, this isn't people will look at information security problems, like things where they want protocol guarantees, and like there is a security gets adversaries.

It's amazing. It's crypto-methodology that involves adversarial thinking and distributed systems kind of thinking. Where like now we get to add this new thing to our toolbox, which is this incentive mechanism design thing. To me, cryptoeconomics is like a mechanism design added to the cryptographer/distributed systems like toolbox.

[0:01:42.3] Host: Right. There's a lot of intersection with cryptoeconomics and game theory. A lot of our viewers are probably familiar with distributed systems, familiar with economics, less familiar with game theory and how it – what interaction game theory might have with something like a distributed system. Can you talk a little bit about what game theory is and how it applies to cryptoeconomics or blockchains?

[0:02:01.2] VZ: Sure. Game theory is a discipline, or like a whole class of methods and approaches for understanding how players play inside the game where they're trying to win or increase their revenue, or basically maximize some payout that's defined in the game structure.

Game theory started with John Nash and the concept of a Nash equilibrium. That's like the most famous concept in game theory. It basically says that a set of strategies chosen by a set of players is a Nash equilibrium, if given that everyone knows everyone's strategies, knowing as it is incentive to deviate individually. So given that everyone's strategies are fixed, like no one has an incentive to change their strategy.

[0:02:52.7] Host: So how does that apply to blockchains?

[0:02:56.2] VZ: Game theory is about predicting how people will behave when they behave rationally, or what kind of situations are possible to behave rationally. Blockchains are incentive systems, as we might want to use game theory to think about how people might deviate from the protocol that we set out, in order to maybe increase their payout, which is itself defined by protocol, at least for a blockchain for example.

A blockchain protocol says, "Hey, make blocks here," and like far as being in the consensus-forming process, and like here is the rewards and the question is like whether people have an ability to gain these rewards by deviating from the strategy and not behaving honestly.

There is like this great paper, selfish mining paper by Gun Sirer and Eyal that showed that – or for proof of work blockchains, like the following protocol isn't Nash equilibrium. Because they show that you could, instead of publishing a block where you found it right away, you could rationally keep it and mine on it a little bit first and you get a slight edge over other people and the protocol, which could turn into like actually prior returns for you. Long and short of it, we can use game theory to analyze and project in our existence.

[0:04:15.8] Host: it sounds like then in the point of game theory to a cryptoeconomic system, you're assuming that the people in the system are basically rational at theirs and they're going to do what's in their best interest, and that possibly they know what other actors are doing. Is this a good way to model blockchains?

[0:04:32.5] VZ: That's what game theory does, right? The thing that we're doing when we design blockchains, we're doing mechanism design. We're designing incentive systems, try to get certain outcomes. The only way that we can really do that is with behavioral models and say kind of what outcome will happen from a particular kind of system.

Game theory is one thing in our toolbox for understanding what behavior might arise from an incentive system. It's not be all end all, but if the thing – it's kind of a red flag if the game theory doesn't work out. We want to have our system be – our system look good under various kinds of analysis, including input.

[0:05:17.2] Host: That makes sense. Okay. Now combining cryptography with game theory is an interesting idea as well. What does cryptography give you that doesn't exist in a normal economic system that you might analyze with game theory?

[0:05:30.3] VZ: I don't think you're really asking me about cryptoeconomics, as much as how does cryptography influence mechanism design and game theory more generally.

[0:05:41.1] Host: Sure.

[0:05:41.9] VZ: For technology is the game theory mechanism I apply to crypto. You're asking me about the vice versa right there that you don't apply to the game theory. It's totally interesting there also, but I just want to be clear that I don't think that cryptoeconomics.

But basically, there's a whole host of incentive mechanisms that may be possible with cryptography that aren't possible without them, due to the limitations of the incentive mechanism, right? At the end of the day, incentive mechanisms end up not being just this mathematical representation, but some program that has to like authenticate messages on the network realistically and in an additional world, right?

Cryptography as being necessary for implementing incentive systems. That said, it may or may not actually end up in forming the design of them, right? It might be more about implementing the design in a way that make sure that the design is carried out as opposed to it being unsecure and the incentives being distributed in a way that wasn't intended by the mechanisms on it.

[0:06:46.1] Host: Sure. I guess my motivation asking that question is I kind of want to build in our audience. Just a intuition for the kinds of things you can do in designing incentives that normally wouldn't' make sense if you didn't have cryptographic primitives available. Things you can for example force people to prove, or force people to give evidence of that. In a normal economic system would just be totally and feasible. Can you give just some examples to build up?

[0:07:09.0] VZ: Those are actually example – those are example or cryptoeconomics a lot of the time actually, where basically you want to do is to incentivize people to provide services in a distributed system and approve that they're doing. That's I think closer to the scope of cryptoeconomics, where you're using incentives to get people to do things for distributed systems.

I mean, in some way people use reputation in a regular economy and also audits, and also to persons that approve that they're doing what they say they're doing to the people who are buying their products. But in our kind of economic setting, we're thinking more about, "We have computers on the internet and they're going to provide services in the market and pay for services at the market," and we want the market not scamming the participants.

We want someone to be able, like if I'm paying for a random stranger to sort files for me, I want to know that they're actually doing it. When that's something that's maybe possible with cryptoeconomics techniques, whereas right now we can be – when you rely on trust in Amazon or Dropbox or whatever.

[0:08:17.6] Host: Can you give us like a really brief example of how something like that might work, a proof that you still have a file that I'm asking to distribute?

[0:08:25.5] VZ: I mean, so that's like a crypto proof. There are crypto proofs with various kinds to show that you have a file. You would basically, you could imagine being paid to produce any one of those proofs at a regular interval. Basically, that combined with [inaudible 0:08:39.8] mechanism, so that people – when you're paying people to store your file, you're not paying the same one.

[0:08:47.5] Host: Look up, what is a CBL?

[0:08:48.6] VZ: You have redundancy. Right, so a CBL attack is a classic problem in distributed systems that has to do with an adversary that spins up a lot of nodes – It's also a problem in reputation systems where an adversary will create a lot of identities.

CBL attack basically means – or it's basically an attack where someone creates a lot of entities to participate in the protocol. In this case, you might want like a whole bunch of people to store your files, because you don't any one of them o fail and then you lose your files.

You might want to say like a bunch of people placed deposits in order to participate in the system observing files. Deposits guarantee that they are the state, because there's some – associated with having a deposit or provide some amount of assuring of their distinct and then their cryptographic proofs can provide a assurance that they're holding the files. That's like an example.

This is just something, like you know, I mean I'm not – I'm sure that if you want to actually go and implement it, there is going to be a lot more details than I have just brought up.

[0:09:55.2] Host: Sure. No. My goal there was just to give our listeners an intuition for just the fact that there are a lot of different things that you can do in a cryptographic, or in a cryptoeconomic system that you just can't in other systems, like they're new primitives that are available to you in designing this kind of an economy that I think are potentially more reliable, potentially more efficient in a limit anyway. It's a new set of ideas that people are thinking through, which is not immediately obvious to a lot of people.

[0:10:22.1] Host: I think Bitcoin is a really good example of this system, which is like simultaneously applied economic concepts to distributed systems and created a whole new host of economic concepts that people are excited about.

Bitcoin is really like an educational tool about both digital currency and what that means for society, and also digital currency, what that means for distributed systems. Both are super interesting, but I like to talk about them separately.

[0:10:55.1] Host: Makes sense.

[0:10:56.3] VZ: Just so that people don't get confused about what cryptoeconomics is. Because I think there's a whole field of people who do mechanism design, and we can't just call all of that cryptoeconomics, because we're using cryptography.

[0:11:08.9] Host: Right. Switching gears a little bit, what is a shilling coin? Can you describe that concept for me?

[0:11:14.1] VZ: Sure. Shilling coin. There's a concept about a shilling game, which basically just means – it's a fancy way to say a coordination game, which is a game where people want to make the same decision, but they don't necessarily have a lot of information about what decisions they're going to make, and so they use focal points.

Shilling coin is just a concept that you could basically have people report on the value, offer some, like external thing if the blockchain are – because they're not coordinating with each other, they will all fairly and honestly report the value and you could pay them if they agree, or pay the ones that agreed more with them – more with each, and pay the ones that don't less or maybe been less.

The idea there is that for using this kind of solution concept in game theory for coordination games, we might be able to secure oracle system for that can provide data feeds, or you don't on a bunch of stuff.

[0:12:24.5] Host: Just to be clear. Why do we need that? Why can't we just directly get that feeds from off the blockchain?

[0:12:30.1] VZ: Well firstly, blockchain isn't – it doesn't have access to data. It's general in the world, like the data needs to be provided to it somehow. If a single party provides it, it might be more questionable. I should say that shilling games are not like a cornucopia.

They have failure modes, like there is – you basically are relying on the assumption that – two of something. One of them is the players can't coordinate and be the players share the same focal point for the true value of a thing. B seems unreasonable, but the first assumption that the players can't coordinate is questionable and becomes more and more questionable over higher stakes games.

[0:13:09.9] Host: Makes sense. Decentralized prediction markets tend to use shilling coins. That's the way that they report on world events. Again to reiterate what you said earlier, let's say they were trying to figure out if Barrack Obama or – not Barrack, I'm sorry. Hilary Clinton or Donald Trump won the election, a blockchain doesn't directly know that, but one way that you can establish this using a shilling coin without having a single party that's supporting on what's going on in the real world, you take a bunch of people who are ideally disconnected from each other and you ask them to try to converge on a value in it, and those who vote for the majority get punished, and those with the majority get some reward, which incentivizes this kind of trust as coordination. Is that a fair characterization?

[0:13:52.8] VZ: Yeah. I mean, that's the intention. That's the intention. The extended to which, it's reliable has yet to be seen.

[0:14:00.7] Host: Okay. Are there known attacks against shilling coins, or these kind of protocols?

[0:14:04.2] VZ: You just coordinate with everyone to just agree with each other on something and it's not true value, especially effective in prediction market, because you potentially get a lot of reward for the market, or everyone sees that Trump won and so everyone was betting – the best change of the market before the oracle reports possibly, right? Then the oracle produce a report wrong and take everyone's mind.

[0:14:29.3] Host: Have these kinds of attacks been seen in a while? Did you know?

[0:14:33.0] VZ: No. I mean, most of these systems are still – I mean A, I wouldn't really know. B, most systems are kind of still too nascent to, I think, have had that enough experience for people to figure out how to gain the system. So that a game comes into the existence, people figure out how to – they start playing with intended before, they eventually figure out how to deviate in a way that benefits them. It takes time for me to be able to figure out how to gain their incentives.

[0:15:00.9] Host: One other concept is what's now is a stable coin. A stable coin is a coin that's supposed to be pegged to some real world asset, such as USD or some unit as gold. How do stable coins work on blockchains?

[0:15:14.4] VZ: Geez. Well, there is different kinds of stable coins. I mean, this cryptocurrency cloud, ROI stable points and there is externally collateral stable points. All stable points basically need to have two properties. One of them is that they can be issued and the other so they can be redeemed.

It basically means that like, oh if you want to buy some of this coin, maybe Sam buying a gram of gold worth of stable coin, basically I need to be able to put money down, put money somewhere. That money needs to do something. Then whenever I want to redeem, I get a grams' worth of gold, worth money out.

There's multiple ways you could work on them. Okay, put the money in, someone receives that money, they go out on the market, they sell it, they buy gold, they put the gold in above, and then when I redeem, they give me the gold or sell the gold. Then I can have this asset.

Another way that it can work is with collateral. There might be – I might be really, like you know pay a price to hold – to have someone – or sometimes they'll actually pay me to collateralize the gold coin that I'm buying.

Maybe you can imagine that I buy a gram of gold, additional token that's worth a gram of gold, and it's got four X that dollar amount of Bitcoin behind it or Ether or some cryptocurrency. Then as long as the price, that cryptocurrency doesn't fall by a factor of 4, then when I redeem there's still enough cryptocurrency there for me to withdraw.

If someone is going along on cryptocurrency, they actually find that quite agreeable, because they think that the amount of cryptocurrency that I've put in will be less than the amount that I take out when I redeem my gold coin. They can basically increase their exposure with cryptocurrency and allow me to hedge and have exposure to this gold coin.

Basically, this is called a contract of difference and the – then all cryptocurrency collateral stable coins can have this property, that if the collateral too much price, then the redemption isn't going to be possible at the full face-value of the gram gold bit, whatever it is.

[0:17:32.2] Host: So how robust do you think the stable coins can be in the long run?

[0:17:36.2] VZ: Well, that's also a very good question. It's hard to say. I mean, I think cryptocurrency collateral stable coins can be pretty robust. I mean, you just have to have enough collateral, but the issue is that that collateralization comes out of a significant cost and that means that they can't actually be that much of it in circulation.

Externally collateral stable coins have all sorts of external risk, like risk that isn't just on the blockchain, isn't just cryptocurrency vice versa. It's risk more to do with things like your ability to get called out and evolve your abilities like buy and sell, both your abilities not have your gold seized by anyone, or whatever assets or collateralizing this coin.

[0:18:14.9] Host: Which seems do you think are the most promising?

[0:18:16.7] VZ: I mean, I think at the end of the day we're going to have all of them, and then you're going to have baskets of stable coins that are like — or stable coins that collateralized by stable coins. So that we have a cryptocurrency collateral stable coins, externally collateral stable coins and people will make stable coins are collateral for both of them in.

Then we end up getting these indexes. That's my little prediction, but at the end of the day basically, what I'm saying is like I think we kind of meet all of them because they're not all like a 100% correlated risk, which means that like in the risk, better to have – better to have more of them.

[0:18:52.2] Host: That makes sense. This seems like a very different risk profiles, but probably useful to have both in the ecosystem.

[0:18:58.4] VZ: Of course. Yeah.

[0:18:58.6] Host: Cool. Well, from that topic I want to veer a little bit to talking about proof of work and then eventually moving on to proofs of stake. I'm going to assume that our audience is familiar with how Bitcoin is secured by proof of work.

But to really, really briefly go over it, so basically the idea of proof of work, also known as locomotive consensus is this idea that there's a sequence of cryptographic puzzles, which have dynamic difficulty. The first person usually solves the puzzle, gets to write the next set of transaction into the blockchain and earns a reward. Is that basically correct?

[0:19:27.9] VZ: Yeah. That's pretty much right.

[0:19:29.9] Host: Cool. Sorry, go ahead.

[0:19:31.3] VZ: Yeah. No, that's totally right.

[0:19:33.3] Host: Okay. Are there any other features of proof of work that are important to understand when thinking about proof of work and the transition to potentially proof of stake? What are the problems with proof of work?

[0:19:43.5] VZ: Yeah. I mentioned one earlier, which is that it's not a Nash equilibrium to follow protocol. That's pretty serious problem, I think, just from the point of view like, wouldn't it be nice to have a protocol where it's actually – and actually deliver to follow the protocol, or even better, a dominant strategy to follow the protocol.

Or even better like us drawing Nash equilibrium and follow the protocol. So basically a Nash equilibrium where instead of individual deviations, like groups of players can deviate together and then redistribute with their payouts to each other.

Then even better than that would be this kind of coalitional dominant strategy, or basically you can get no matter who you're including with – it doesn't matter what anyone else is doing, your dominant strategy's default protocol.

That kind of thing, really, really nice. But you can't really get it to work, because of limitations of future work. Some of the limitations are actually fundamental. Like the fact that you can do self-mining isn't fundamental, because they make work architectures that don't have that problem. But the fact that say a majority of the hash power could sensor blocks is something that is going to be necessarily true in all proof work systems and isn't going to be necessarily be profitable.

Because proof of work can't really tell who is meant to be since we've walked – sorry, who is meant to be producing walks. They can't really tell when blocks are missing. At least, they're traditional, anonymous, outsourceable for work for anyone who can produce the proof of work.

There are proof of work systems where you specify identities that have to produce the proof of work, but those starts to look more and more like group stake systems. But anyway, so what I do is – what I was basically just saying is Nakamoto consensus, Bitcoin's protocol doesn't reach all of the optimality that we can imagine, in terms of mechanism design and game theory.

Additionally, it doesn't have some of the steps that we want from consensus protocols. So a consensus protocol, but it doesn't have any kind of notion of finality, any kind of notion of the fact that blocks will never be averted. I mean, it kind of does. It has a little proof that they were reverted, but that only holds if in a partially synchronous network.

[0:21:55.3] Host: Sorry, can you elaborate a bit there?

[0:21:58.7] VZ: Yeah. There's a couple of things. Firstly, let me say that when the Bitcoin works is that if you ever – everyone try to hash in this blockchain and you to add a proof work to it, never affix the proof of work watching with the most work.

If someone were to produce it before watching with more work, that doesn't include in some walk, then that walk would like it's suddenly be gone from history. That kind of reversion doesn't really happen in traditional consensus protocols, but there is like this proof that there is this proof that Satoshi gave, that if there's luck, less than half of the – sorry, the mining power the dishonest, then that won't happen.

Now that proof relies on an assumption about the rate at which walks propagate and the radar would people find locks. This is what I was referring to with partial inquiry, there's a great deal of research and consensus protocols to try to figure out how to reach consensus without making, or like have consensus in a safe way without making assumptions about timing.

Whereas, proofs of Bitcoin and proof of work is a partially synchronized protocol, which means that it makes some arguably pretty weak, but still some pretty significant timing on something. I mean, the whole idea of a hash rate is a very synchronous thing, right?

The fact that we have a block times every 10 minutes is a very synchronous kind of thing. Those are the things that traditionally we don't necessarily want in a consensus protocol. Normally what we want is something called asynchronous safety. Which means that no matter how crazy people's clocks run in the future, no matter how fast or slow people's clocks is determining, no matter how fast or slow, and this message is got across the network, we still have the property of this walking that could be reverted.

That's something that you just don't get in proof of work, because proof of work is not asynchronously safe. It's always going to be the case that walk can be averted if someone was able to run their process arbitrarily fast, because then they can just do more proof of work.

[0:24:00.2] Host: My understanding then is that another way of saying that is that the only guarantees you get in a proof of work system are probabilistic. There is no determinants to guarantee that the block is definitely final, and someone shows up later with a longer and better history than the block goes away and there's no block that's exempt from that.

[0:24:17.1] VZ: Yeah. I mean, you are exempt from it if you're willing to admit certain assumptions about hash rates and timing.

[0:24:25.9] Host: Sorry, can you go into more detail? What exactly do you mean?

[0:24:27.1] VZ: Yeah. I mean, if the network latency isn't arbitrary – isn't arbitrary, I mean if message arrival isn't arbitrary, but message arrival then some bounded time, even if we don't know that bound. If hash rates where you know there's no bounded, we don't know that bound. Then if we wait enough walks, we don't necessarily know what enough is, we won't gear for. There's a proof that shows that.

[0:24:53.2] Host: Interesting. Okay.

[0:24:55.5] VZ: All of this says like, "Things, we need founded times, time outs that we did, hash rates." Sorry, bound and network propagation and bounded hash rates in order to guarantee that if we wait enough, block will be over.

That's secret or something that's required for both the safety and liveness of the one. Bitcoin is a extensive protocol and it's an incentive mechanism. It's an extraordinarily simple consensus protocol and extraordinarily simple incentive mechanism. It doesn't do a lot of things that we want from both ends and to mechanism and a consensus protocol.

Which I think is not actually as surprising given how remarkably simple it is. But it's an extremely good pedagogical tool in my opinion. It has its own. It's on a huge amount of value just by putting these two things in the same place; the incentivizing and the consensus.

[0:25:50.5] Host: I'm sure the Bitcoin nationalists will be really excited to hear you describe Bitcoin as a pedagogical tool, but I understand what you're saying. Let me ask you, so it's commonly described that the miners in a proof of work system play the role of securing the network. I think to a lot of people, it's not really obvious what exactly that means and what sense their security network. Can you flush that out a little bit?

[0:26:15.1] VZ: Yeah, sure. Miners do work in order to secure the network. What that means is basically they add work to the blockchain in order to make it tamper-resistant and make it hard, so much reverse the blocks.

From mistake, there's like a different system. Instead of doing proof of work, we're going to somehow use coins in the protocol, like actually Bitcoins you can imagine, or ether, or some kind of token in order to create this tamper-resistance, this difficulty to an adversary to attack the protocol.

Just take ideas that the adversary would have to actually buy tokens and attack a protocol at their expense like that, and proof of work they would have to buy mining power and attack the protocol at their expense like that.

[0:27:00.4] Host: So this is a good time I guess to get into proof of stake. What exactly is proof of stake? Can you just describe end-to-end how proof of stake works?

[0:27:07.7] VZ: Well, I mean, firstly proof of stake is a wide design space and it's hard for me to describe and then how it works, because I'd have to describe how this will work and then how you could possibly take to Bitcoins, and that's a lot. However, I can describe to you the history of proof of stake. Maybe it would help.

[0:27:29.4] Host: Yeah, let's go with that.

[0:27:30.5] VZ: Proof of stake started off on this great insight, with this great insight from this guy named Sunny King, who realized that like maybe we could simulate miners by buying coin instead of hardware and putting the coins to work.

Then this is the thing that led to the birth of PPCoin, which is the first stake coin. Then proof of stake, it's always have been – I mean, this weird voodoo magic thing. It was at the time a weird voodoo magic thing, where like somehow just like this crazy mining process that everyone was used to participating in to mine Bitcoin. It's very really by hardware, you put in the wall, pay your electricity bills to earn your coins, sell your coins to pay the bills.

You have this proof-free like clear economic game. It's like a water that ends up being really capital intensive. Proof of stake, instead you would like just buy some coins and put them in something and it doesn't necessarily consume that much electricity and somehow it seemed weird, right.

There was a bunch of variations on that, PPcoin iterations on improving some of the problems that people noticed with it. Namely things like, for example if you made a bunch of walks and you chose the blocks right, you might increase your probability of getting a block, being chosen for a block later.

There was basically the sink hole, and not to get state attack, or not to get state problem where you had an incentive to create walks and all for just in case add some fourth one. Whereas again proof of work, you can't – every block costs a lot of work, so you got to be really careful about where you put it.

There is this thing called the long ridge tact problem, which basically said that someone could buy old coins and use the old coins to – coins that I mean, cryptographic keys to coins that no longer held all those keys, and use those to conduct an attack from a more walk – it's like further back, in order to make a chain that's longer and therefore will win in this kind of four-choice rule thing. Because back then, proof of stake really was just trying to emulate proof of work.

Then I think the main shift that happened between the bad era proof of stake and what I think we're coming into now like a modern era proof of stake, is a shift from using coins as risk-free simulated miners and trying to make it difficult to gain that and have it work under a majority honest assumption.

Is that we're now we're moving toward where we're at least I had Ethereum and does with the other projects theme, but using security deposits rather than just collect free coins. It is more like, you place deposits and then you participate in a consensus and if you do it, if you behave [inaudible 0:30:19.6] way, you may lose your deposits.

As a result, that nothing at stake problem was addressed because you had this deposit instinct. That is a long-range tact problem, which all sounds very similar to have a solution, or basically you never trust signatures from coins that are no longer on deposit, because like only depositing mean anything.

That led to this change in the trust model where basically rather than authenticating everything from the Genesis rock in the south of proof of work, kind of need these tabs and recent information about who currently has deposits, or some hash that you use to verify proof back with deposits, in order to authenticate the chain.

The history of proof of stake, I think until about 2014, as far as I – maybe early 2015, then which you have to see that – would just realize it, “Oh, let’s use security deposits.” Doing incentive mechanism design for consensus protocols is really a difficult thing, because consensus protocols are actually really complicated and they’re the world of consensus protocols that existed before Bitcoin and look nothing like Bitcoin.

There is really a rather complicated protocols and research that explored the stuff and where they didn’t really think about incentives at all. I think like the last three years, we’ve been really working hard understanding consensus really deeply and building consensus protocols that can be incentivized in a way that’s natural and that could be – works from both sides, from the point of view like well you know that consensus and also from the point of view of the mechanism side. I could go boring to that, but I think it’s already gotten to a point where it’s quite technical.

[0:32:18.8] Host: Sure, sure. I mean, this is a technical podcast, so I don’t want to shy away necessarily from details. But one thing I guess to – so just to also frame for those who are not familiar with Ethereum, so Ethereum right now is a proof of work-based system.

There is a plan that – I don’t know these item and I’m guessing the next year. To move Ethereum from a proof of work-based protocol which it currently is to a hybrid proof of stake proof of work protocol and eventually to entirely proof of stake, is that correct?

[0:32:45.6] VZ: Yeah. That’s correct. Yeah.

[0:32:47.1] Host: Right. The first thing I guess I want to ask you is that for the network the size of Ethereum it seems like quite a risky transition. What are your thoughts about managing the risk of moving from proof of work to proof of state?

[0:33:00.6] VZ: Sure. I mean, there's a bunch of different types of risk. I mean, there is kind of – I mean, the thing that some reasons are going to be worth to worry about, but I mean like myself and Vitalic, or the main people who really are pushing this and Ethereum.

By the way earlier you said I always needed a proof of stake. It's really myself and Vitalic really work together on this. It's not really like either us or really like a true leader, I think. So there's like this kind of like firstly, there is this fundamental technology feasibility risk, which we're not really concerned about at this point.

There is implementation risk, which is definitely somewhat concerning, because the protocol isn't – it's pretty simple, but also pretty complex. It's complex enough where you could just use some software implementation problems leading to actual risk. So obviously we need to make sure that A, the spec is crystal clear and correct. B, that the implementation that we match the spec in aren't and are compatible with each other. That's a lot of work.

But actually, I think the biggest risk for moving from the stake isn't any of this. It's actually a more political risk on the rest of people being upset at change just because they don't understand it and because they A, are minors or B, are Bitcoin maximalist.

Any of our suspicious proof of stake because they heard about and I mean, you've got nothing at stake along the tech problems from the chromosphere for years. I think there is this educational/political risk. I say slash, because it's really I think education would go a really long way, but I also think that there's an extent to which people's incentives is mean that like education is not really going to solve everything.

But still, we think that proof of stake is really important from the point of view of increasing these ability of security and efficiency of blockchains. Also from the point of view of its place on the scaling roadmap, because blockchain's charting is actually considerably less effective if you were a short consensus with what work.

[0:35:03.1] Host: Charting is one of the pieces of also the Ethereum roadmap and scaling. But that's very challenging to do without moving the proof of stake, correct?

[0:35:11.5] VZ: It's very hard to sample miners and validators to particular shards. I think they're responsible for them without proof of stake.

[0:35:19.0] Host: Right. As you mentioned –

[0:35:20.5] VZ: Basically because you need to go to [inaudible 0:35:21.5] proof of work and gauge people's mining power and then assign them to shards in a non-outsourceful way. It is just very different from the proof of work model today. At that point, you end up moving so much into towards for sake of all of that; you might as well. You might as well just didn't sit in.

[0:35:40.3] Host: Right. You mentioned though that proof of stake increases both the security and scalability of Ethereum. Can you go in to explain why exactly that is?

[0:35:40.3] VZ: I said security usability and efficiency.

[0:35:51.1] Host: Security usability and efficiency. Sorry, could you explain why that is?

[0:35:55.6] VZ: Sure. Security thing, I mean we can talk about it on a couple ways, but basically you have better economic analysis. I mean, it's going to be like following the protocols, actually a meaningful room and we're going to have ability to show that actually you have to be profitable to attack the system, or you can attack the system and be profitable, like you can and like say for a work system with like a majority coalition.

Also we're going to have things like finality where you'll actually be able to have at some point where you can say, "Okay, this block is not going to be reverted in a way that is asynchronously safe." That's nothing to say not possible proof of work there. It's like a security benefit, which very much mirror the conversation you're having earlier.

Then there is the usability aspect, which is basically lower latency. You can actually tell how much secure you're getting if there's a partition, like you immediately see that you don't have all the hash power, or sorry, all the staking power, you like know how much security you have much more clearly than you would proof of work.

I mentioned latency, that's actually a pretty big deal for Ethereum and for blockchains in general. It turns out that people really like fast confirmations for their transactions. Then there is the efficiency question, which basically by that I just refer – I'm referring to things like the amount of the dollars, the total fees ,and issuance spent for security, and the total amount of compute network overhead that the blockchain actually uses.

Right now you have to imagine that there is tens of millions of dollars every day going into mining hardware – I'm sorry, into miner's hands, going into paying just the bills, like huge rigs. That's a really high-cost economically speaking. That's like, when I say high efficiency, I mean both that cost of the dollars and also in terms of the bandwidth computer has. We can get I think more security, usability at a much lower cost. I think it's the end of the day and have three big no brainer.

[0:38:01.5] Host: Right. I remember reading figures along the lines of that the Bitcoin network every day uses much power as I think the country in Nicaragua, they're actually outdated at this point. But it consumes an enormous amount of energy. As far as proof of stake, as orders have emitted less in its energy consumption for the same level of security guarantees.

[0:38:24.0] VZ: Yeah, of course. Same level of security guarantees, you have to do and use and give a security model, but I absolutely agree and I talk entirely about all this work.

[0:38:31.9] Host: Sure, sure. One thing that's interesting, so there are a lot of other blockchains that already are using proof of stake. Can you talk about a couple of them and maybe if you've received an inspiration or had any obviously, like – and be looking at comparables and try to see what's working right now and what the weaknesses area for current proof of stake implementations. How is that going and influenced those other than Casper?

[0:38:53.4] VZ: Yeah, sure. I mean, firstly one of my biggest influences that are built on Casper and other proof of stake protocols is I at least got two of them. One of them has been abandoned right now, but the other one is still kind of chugging along on its way to production.

The second one is tenerant. Tenerent is this proof of stake protocol that Jake Barn, and now Ethan Buckland are working on. Basically it's a traditional consensus protocol that finalizes every walk and before it makes the walk. So there is never ever forking and it's asynchronously safe and it uses security to cross-visit and people will lose their money if they are caught being visiting.

It's basically an application. It's basically taking – I just think it's in this protocol, modifying and some finding a bit, then applying very basic mechanism – very basic security deposit incentives on top of it. Another thing that inspired me is Dominic William's paper on Pebble, which is like a product – I think he since abandoned, which also high like security deposit-based quorums and you have –

It was basically like, those are really cool because the real first sharding thing and also one of the first security deposit base thing that I look at. Now Dominic Williams is working to affinity and there are a whole host of different ideas. I'm sure that he's still going to be working on proof of stakes eventually, but I'm not sure if that's pretty staying right now, not to state on his stuff.

Other than that, there's the classic peer coin next, you know, coins that, you know, I would say that didn't do – aren't doing a lot of the mechanism design stuff that I really have come to expect. But instead, but do have very blockchain like this for those. Unlike tenerent or Pebble, which have more traditional consensus protocols, which finalize blocks one at a time and there's never any forfeit.

I like both of these approaches and I spend a lot of time, have spent a lot of time [inaudible 0:41:15.5] them. I believe I've been successful, where basically I have a blockchain forks and I get the same type of finality in the end, that a traditional consensus protocol, some traditional consensus protocol gets.

[0:41:28.6] Host: You and Vitalic both had some very vocal critics in the community who claim that Casper is very unlikely to be secure. Let me ask you, what do you think are the best arguments against Casper?

[0:41:41.9] VZ: Interesting. Geez, it's too hard to understand. I mean, I think it's probably the biggest one, but I think it's something where we're really making a lot of progress defining things, making it here. I think the complexity is probably and the main thing that I think I can understand why people are turned off by the complexity of proof of stake.

That said, I mean the simplicity of proof of work, I guess I'm realistic. In terms of fundamental criticisms that people have, is that they like – people really worry about this change in trust model that I talked about earlier where I mentioned, instead of finding most work from the genesis walk, we'll use like a piece of recent information to authenticate the state and this changes the trust model so much, because you need to actually have – you need to actually have someone inside the network that you trust to give you a piece of information for you to authenticate.

It's like the [inaudible 0:42:30.2] has a public key that changes over time and you just know what that public key is to sending a message, or to even listen to it. That is a direct change in the trust model, which we kind of have to accept and move to for the stake world if we want to have good mechanism design.

People aren't uncomfortable with that, understandably because it's an additional point where I might fail. However, we caught weeks of activity and because this week and it's that like, it's something we only do once and the moment you have this information, as soon as you have this information everything else is objected.

It's like you get public key ones and the process by which you update it in the future, you can kind of do objectively just by yourself without trusting anyone. The fourth trustable is entirely objective once you have this piece of recent finalized information about to security deposits.

I think that actually we sacrifice a little bit on the objectivity with this kind of piece of information that's required to authenticate things like this, but we gain a huge amount, namely like all the benefits I talked about earlier in return. So I think that's a good trade, but aren't comfortable with that.

People are concerned about proof of stake being wealth-centralizing, but I think that's really crazy concern, because I mean we've seen proof of work, become extremely centralized and the main benefit of proof of stake actually is that it makes impossible to hold the players to a better – more to account, which is why we're able to get better like we came through in kind of properties.

There's more accountability of proof of stake, proof of work, and they both have the same amount of concentration, then I think it's a no brainer to go stake. People think somehow that because proof of stake is more directly bonding than miners, which have to be bought with money and maintained with expertise, that proof of stake is less – because I'm out and more concentrate.

But I was saying, even if that was true, the fact that more accountable because the protocol has more access to it, it really does have more than compensate for the kind of more concentration. I mean, there's basically – it's one thing to think about the concentration of power in the game. The other thing about like what the rules of the game actually can do to constrain the use of that power.

My claiming is that like we can do way more constrained abuse of power in proof of stake. That is possible before. Also I happen to believe that in proof of work, especially with ASIC, you end up having extreme concentration.

[0:45:02.8] Host: Can you go to the detail what do you mean? First, can you define what an ASIC is and then what's relevant to discussion?

[0:45:08.9] VZ: Yeah, ASIC is an application-specific integrated circuit. It's specialized hardware. In Bitcoin, there's been this trend of building ever more powerful obligation-specific in a circus to basically solve these triple problems in order to mine Bitcoins.

There is a small number, I would say like two get that of ASIC manufacturers that make chips that are performance enough over the – to put a dent in the total binding power and again that can really, I'm going to say there is one or two ASIC manufacturers that supply future – will basically produce the future hash problem.

Your enrichment and your relationships with these people determine your ability to succeed as a miner, because you can't get with as chips, and everyone else does, you can't get the has power in the future. That creates tremendous centralization.

There's been efforts in proofing of work to do ASIC resistance proof of work, which has led to a lot of GPU minable coins, because GPUs are actually are already kind of ASICs in a way. They're already super specialized chip with a task. If you could make a hashing outgrow them, really suited that, it's hard to get much of a gain by making an ASIC just for that.

In this case, luckily somehow, unluckily somehow depending on how you think about it, irrespective is instead of having these two Bitcoin in the same manufacturing companies, we have like MD and Nvidia, be even then ultimate beneficiaries along these block awards, as you buy them at a hardware in order to participate.

I think the fact that, you know, there is like this – I think the concentration of power in the supply chain for minors is like worse than the concentration power in terms of coin ownership. But to some extent, that's just my opinion because in both cases, with ASICs or GPUs, it's just two companies. One of the Bitcoin mining company is definitely is the underdog and MDs or really a lot exist, because of – and tells them to trust concerns and things like that, or seems to be.

[0:47:29.6] Host: If people had already uses e-hatch for its preferred accounting, which is ASIC resistant, correct?
[0:47:34.1] VZ: Yeah.

[0:47:34.8] Host: How much centralization is there in Ethereum mining right now as a result of being ASIC resistant?

[0:47:41.4] VZ: I think that there is much less centralization in Ethereum mining, because of ASIC resistance. However, if people are from freak out because of the mining pools, better things kind of important to realize, like ultimately at the end of the day the distribution of cards that matters, not the ownership of mining pools, because mining pools for now anyways don’t have walk-in. If they do view the trust, people will just mine another pool.

It’s hard to measure the business realization of these things, because you really need to face and go out and do legwork and find who has what graphic cards is mining, and but people are already private about this stuff. It’s not the case that every miner is advertising what they’re doing.

[0:48:19.7] Host: All right. Cool.

[0:48:20.5] VZ: Some miners are mining in countries where it’s like illegal for them to be doing it and they’re doing it as a way to preserve their capital turnout, just to save money or whatever.

[0:48:31.5] Host: Makes sense. Cool.

[0:48:32.2] VZ: It’s hard to say, but basically GPUs are more widely accessible than ASICs.

[0:48:40.9] Host: Right. I want to veer the conversation one more time to a final topic, which is kind of about all the stuff hype craziness that’s going on right now in the blockchain space. Now you’ve come out on your blog and on Twitter as being very cynical, I guess I would say about the mania right now around Ethereum and ICOs and blockchain hype in general.

Let me just kind of give you the floor for a second. How do you feel about the hype that’s going on right now surrounding Ethereum or blockchains in general?

[0:49:07.9] VZ: Basically I have a bunch of reservations, because I think that the interest, commercial interest in the technology has can refer our pace, detect in the academic understanding of it. A lot of people think that’s like a great thing in some ways and I think it is too in some ways, because it’s exciting and we’re learning a lot really fast, because there’s a lot of interest in something that we don't know that much about. But also, I think people are putting the carrots ahead of a –

[0:49:39.0] Host: The cart before the horse, I think is what you're looking for.

[0:49:41.0] VZ: Cart before the horse. Yeah, yeah.

[0:49:43.9] Host: The carriage before the steed.

[0:49:46.3] VZ: Yeah. Basically people are being reckless, because of the exceptional returns that they have experience through the currency, because of the incredible amount of excitement. We see this thing where a lot of our cryptocurrency projects are essentially communities around an idea, which I think in some way quite interestingly cool, because sometimes these ideas are really cool and there's a lot that can happen in the community that's really excited about an idea.

Instead of making change, people could become understanding ideas because to find out that actually a lot of the stuff is just done, solved by this one simple idea and then a lot of projects they're useless. There's a lot of stuff that could happen where a lot of people's investment, hopes, could be dashed just because of – like all the crazy uncertainty and an unknown information and stuff that is all over the place.

I mean, that information symmetry in the spaces is incredibly worth knowing, that the information that the market pays attention to and the information that the market pays attention to, and the information that devs pay attention to is entirely different, like the miners, the businesses –

I mean, everyone lives in the wrong world and it has very different experience and a difference in space is really remarkable. All those kind of information and symmetry on certainty, combined with huge amounts of excitement in investment makes me concerned, right?

Especially when I go to random parties and I hear people talk about how they're buying Litecoin or whatever, you know whatever cryptocurrency that I've never heard of. Or how they've bought ether and it changed their life and they have – These crazy stories from people who, given the state of the technology or early stage, I am not sure – maybe I'm wrong. Should all be – I'm not sure that the ecosystem is ready for the amount of interest that it's getting.

But maybe, you know the argument goes that all that interest makes it more ready. The investment makes push things faster. Everything happen a little bit faster, because it needs to, because it's lots of people coming in and they're losing their private keys, they don't understand what crypto-credentials are, like they want to know what the – they're asking for their password and there is no login to the service, because it's like a crypto service.

All of this is huge amount of education and safety for regular users who aren't like cryptocurrency specialists, that like it doesn't really exist there and people lose money, like all sorts of crazy ways. It's sometimes it's quite sad, right? The tech end of standards, norms, a little bit of a kind of mature software, just isn't really there yet.

[0:52:55.0] Host: Yeah, you twitted earlier Ethereum isn't safe as scaled, what is immature tech. Having attempted to develop on Ethereum and its solidity I would have actually have to echo that sentiment. What do you think of the way that people are treating the blockchain now and how long do you think people take until that changes, like how long do you think it will take until Ethereum does become mature in something that you could sort of comfortably point an average user towards and say, "Hey, this is ready for you now."

[0:53:21.8] VZ: Yeah. I mean, that's a great question. I think that there is a whole bunch of things that need to happen for me to get that point. Because when you say average user, you're really talking about millions and millions of people, at least and potentially. I mean, let's say.

That one we're talking about scalability, the safer higher level languages, like the things that give you lots of warnings when you're doing something that's not good practice. Those stuff is coming – it takes time. I think basically developer kind of tools, culture – Yeah, I think cases like developer tools and the watching and scaling are the main things that hold it back. I don't feel super, super duper strongly about my answer, so it might change my mind.

[0:54:16.8] Host: Sure. Fair enough. Then do you remember if I didn't ask you at least once, so what do you think about the ICO mania that's going on right now? Any overall higher level thoughts or predictions about what's going on in this phase?

[0:54:31.6] VZ: Yeah, sure. I mean, I think that basically a lot of people are realizing that raising funds with ICO provides a lot of benefits, compared to raising funds with DCs. Primarily affecting you don't need to structure your entire business and operation and vision and plan around what DCs expect. But there's costs also.

It's also like – it seems very easy to raise huge amounts of money. But there are cost, there is regulatory uncertainty about the nature of these things. Are they securities? I mean, sometimes certainly seems so, sometimes it seems less so. The SCC has a pretty clear mandate about securities and the investing public, versus the general public. That's one side of the story obviously.

The DOs part of the story in terms of actual products that are being funded with cryptocurrency – sorry, with these ICOs. I would say that it's like a mixed bag and probably like not that different from normal startup success and failure rates.

Maybe actually, you would argue that they have a lower failure rate than startups, because their currency community is formed around projects at ICO and someone from that eventually would probably pick up the slack that the founders leave, which is less likely to be true in a startup.

For the most part, I think that – I mean, ICO is very questionable because I mean, a lot of this tech I think is incredibly difficult to build STP. A lot of the times, people are coming in thinking that things are going to be much easier than they are. But sometimes, I am pleasantly surprised by people who have simple architectures that aren't trying to do too much crazy stuff and seem achievable.

That said, I often do things that people think are – seem unachievable, some maybe I shouldn't judge too much. But basically, I think ICO in some cases have been and are a really good thing, that front of great projects that build communities and large group of stakeholders who participate in this share thing together, and have –

I think that there is also cases where that the people who raise the money maybe aren't that good at managing all community thing. Maybe there upside expectations, maybe people will leave, maybe there is like drama, maybe there is a thing. I mean, stuff fails all the time. Cryptocurrency is not an exception.

[0:57:11.6] Host: Right. Well, yeah. I think it's definitely completely nuts right now. It seems to be something of a frenzy, but I agree with you that it seems like that there are both positive and negatives to what's going on right now in ICOs. Certainly, even if things right now are unsustainable, eventually they'll fall back into an equilibrium.

What do you think is the sort of a longer term, what do you think is the effect of all these ICO and the awareness of the public of ICOs going to have on the blockchain ecosystem?

[0:57:42.4] VZ: Yeah, it's interesting. I think that when something is funded with an ICO, it's much more likely to contain a token. I think therefore, the public ecosystem will involve in any more tokens than it would have otherwise, which I think actually is not necessarily a positive thing. I think lots of apps that integrate maybe should just not integrate them and have the tokens represent like an emotional connection to the project or a reward point, or something that's more – more nebulous rather than tied into the project at every level, at every possible opportunity.

People like integrate their tokens into their applications, because it gives the token buyer some assurance that there's going to be a reason for people to buy them in the future. But that doesn't necessarily always lead to I think what I think is the best design. I think that's actually my biggest problem of the ICO space, is that I think lots of people are just taking products that will be great without tokens, adding tokens to them and making them less great products.

On the other side, lots of people making lots of money on ICOs and finding lots of stuff that maybe otherwise wouldn't have gone and built at all. So it's hard to waive those things against each other.

[0:58:48.4] Host: Yeah, makes a lot of sense. Well, Vlad. It's been a really fascinating conversation. Thanks for taking the time for chatting and I look forward to seeing what happens with Casper.

[0:58:56.9] VZ: Okay. My pleasure. Safe patients, it's going to happen soon.

[0:59:01.9] Host: Awesome. We'll do. Thanks so much for all the hard work.