Demetri Kofinas: What's up everybody? Welcome to this week's episode of Hidden Forces with me, Demetri Kofinas. In this week's episode, I released the audio for my exclusive sit down video interview with Leemon Baird, the inventor of Hashgraph, ahead of the now completed launch of Hedera, a revolutionary public ledger built on [00:00:30] top of the Hashgraph consensus protocol. Hedera implements a suite of solutions that we have never seen before in a public ledger. Its approach to governance is unique, its anticipatory attention to regulatory compliance, preemptive. And its innovative perspective on the question of open source versus open review challenges the paradigm that has come to dominate the first 10 years of software development in crypto economies and distributed Ledger technologies.

In our first [00:01:00] two interviews in the fall and winter of 2017, Leemon tackled for us the problem of consensus and how the Hashgraph team has attempted to solve it with unparalleled levels of security and performance. In this episode we explore how they've managed to scale it. How does Hedera protect itself from Sybil and DDOS attacks? Against those responsible for validating the ledger and processing transactions? What is so unique about Hedera sharding implementation that [00:01:30] allows for smart contract execution across multiple shards, processing hundreds of thousands of transactions per second at near zero latency.

Is it possible that we may have finally arrived at a solution to scale for distributed consensus that allows for the development of software applications with real multi-billion dollar, even multi-trillion dollar use cases like ride sharing, file storage, stock exchanges and micro-transactions? After 10 years [00:02:00] of excitement, development and aspiration, is the evolution of distributed consensus finally upon us? Might this be what the second internet revolution actually looks like?

As always you can join our email list by visiting the show's website at HiddenForces.io. If you listen to Hidden Forces on your iPhone or Android make sure to subscribe. If you like the show, write us a review, and if you want to sneak peek into how each episode is made, or for special [00:02:30] storylines told through pictures and questions then like us on Facebook and follow us on Twitter and Instagram @HiddenForcesPod. And now, let's get right to this week's conversation.

So Leemon, it's great to be able to have you back on the show again.

Leemon Baird: Oh, thank you. It's great to be here.

Demetri Kofinas: I'm very excited for the news you're going to share tomorrow. We're filming this one day before your public announcement for the public ledger. And that's what we're here to talk about today. There will certainly be people [00:03:00] watching this who are not familiar with Hashgraph or with the consensus protocol and we'll have an opportunity to get into that of course as part of this question that'll come up. But I want to begin with really Hedera, because that's the big news, that's what really on everyone's mind.

In your vision statement in the white paper you emphasize openness, speed, fairness and stability as being sort of central to the architecture of the public ledger. [00:03:30] Let's begin with openness. The block chain community uses something known as open source, a development sort of model of open source. Hedera is open review, what is the distinction and why is that important?

Leemon Baird: Yes. So you want to have transparency, so everyone knows what's going on, but you also want stability, you want to be able to trust that this isn't going to split, and you're not going to have infighting that causes all sorts of problems. How do you balance [00:04:00] that? How do you get both? How could you have stability and have transparency at the same time? So the thing that we do is we have good governance, 39 major players who should be able to understand how to manage an ecosystem, the economy, the code base all of those things, good governance. But we want to trust but verify.

We don't necessarily trust any individual, we don't want them to trust each other and so one of [00:04:30] the things that we want to have happen is that everyone can see everything that's going on. And so the network itself is running on nodes all around the world. We want to scale up to millions of nodes around the world being run by ordinary people. Any person can do it, they can do it anonymously, they can do it anytime they want, and they are running the software.

We give them the source code, anyone in the world can see the source code, they can compile it and see if it matches the compiled code [00:05:00] that they're running, or they can compile it and run what they compiled, and so that we have complete transparency, the network is made up of nodes like this, so if it were, when we're all running the same software, and we can see that we actually work, we actually operate with each other, we all get the same assigned state, which means that we have strong cryptographic guarantees that we're all doing the same thing, absolutely strong and so it's impossible for the governors to slip something in that we can't see.

Demetri Kofinas: So you have complete access to the code.

Leemon Baird: Complete access.

Demetri Kofinas: You can see everything, you can recompile [00:05:30] it if you want to.

Leemon Baird: You can recompile it if you want to. In fact, it's a good idea to do so just to make sure that we didn't slip something in. And so we have complete access, complete freedom to see what's going on, to understand what's going on, to catch anything nefarious going on, which makes nefarious things less likely because you're going to be caught.

Demetri Kofinas: It's not a black box.

Leemon Baird: It is not a black box, that's it. So this is open access, this is transparency, this is ... Everybody runs nodes, they are running the network, they [00:06:00] don't trust each other, no one has to trust the 39, but the 39, the people governing it, can govern. And so it is not open source, if it were open source that would mean not only can you see the code and use it, but you could legally stand up another network and confuse the market. No, it's not open source, so we prevent that to try to keep it from splitting.

Demetri Kofinas: I mean what you're touching on right now, you're talking about governance, I mean explicitly obviously you're talking about stability too, which is part of that, [00:06:30] and the fact that in block chain communities governance has been a real issue because you can have forking and also there are a lot of incentives around wanting to monetize your own protocol, and the best way to do that in some cases is to fork the protocol entirely. Okay, so we're going to get more into that when we talk about sort of technical controls and controls in general and governance, which I want to get into.

Let's get into what I think is the most sort of phenomenologically impressive aspect of Hedera and Hashgraph, [00:07:00] which is something we've covered in the past. I found it at least to be true. I think you say the same thing when you speak with enterprise clients for permission, the use cases of this technology and that is performance. We've talked about it sort of in abstract terms, or in some specific terms about hundreds of thousands of transactions per second, near zero latency, but you have now empirical data and results from tests you've run on servers located within hundreds of miles, as well as thousands of miles of each [00:07:30] other.

What can you tell us about those results? What can you tell us about the performance that you've seen and then let's talk about how you think that's going to scale on a public ledger and how you expect it to scale with Hedera?

Leemon Baird: Sure. Performance is not a number, it's a whole bunch of numbers. And you should download our paper and look at the numbers, you see graphs, you end up with an infinite number of numbers in some sense, that's really the better answer. But I can just tell you what I'm going to say tomorrow night is just a few scenarios [00:08:00] of the many scenarios we tested. So for a national or worldwide credit card, you might find and what they typically say is on average they're doing 2,000 transactions per second, that's on average.

But then sometimes it has to burst, peak up to over 50,000. And the requirements are that, when you swipe your card you have to have this completely approved or rejected, completely done in seven seconds. This is the requirement, [00:08:30] on average 2,000 maybe bursting a little over 50,000 and then point seven seconds of latency or of time to finality or of consensus time. Of course, consensus is easy on the server but that's what they do. So that's the bar that they have set for us.

So can we do that? Well, when we have ... For example if our governing members are running notes, that many notes spread around the world, if we run at 50, [00:09:00] 000

transactions per second, not two thousand but the 50,000, not as a peak but as just all the time, we see this finality in 2.9 seconds. That's what we see. This is running it on Amazon nodes, AWS nodes around the world.

Demetri Kofinas: This is globally. This is globally distributed network we're talking about right here.

Leemon Baird: This is global. So this was running it in Tokyo and Canada and Australia and Frankfurt, Germany and Seoul, [00:09:30] South Korea and Sao Paolo in South America and on both coasts United States, eight places. This is what Amazon calls regions, so eight regions. You see 50,000 transactions per second, steady-state not just peaking but steady-state forever at that speed, just a couple of seconds, 2.9 seconds of time to finality or latency. And this is not time until their confirmation, some systems have a confirmation, and then you get another confirmation, and another one, each one makes you a little bit more [00:10:00] sure, we don't have something like that. I'm talking about time until you are 100% absolutely positive.

Demetri Kofinas: Well that's the Asynchronous Byzantine Fault Tolerant Consensus.

Leemon Baird: You got it.

Demetri Kofinas: And that's because ... So why don't we talk a little bit about that for people that are coming to this technology for the first time or who need a refresher or reminder and what's so unique about Hashgraph and the fact that it actually does reach consensus versus some of the alternatives which do not.

Leemon Baird: Absolutely. And if you don't mind, I gave one scenario, I don't want you to think that we're limited to a [00:10:30] mere 50,000 transactions per second.

Demetri Kofinas: Well, I've seen up to 500,000 or [crosstalk 00:10:36]-

Leemon Baird: You gave away the punchline, exactly. So 50,000 transactions per second, 2.9 seconds latency, this is around the world, what if you didn't want to do 50,000, I mean if you want to do 100,000, you just asked to do double. It does it fine and your latency goes up, by less than half a second. You go to 3.4 seconds. So the latency goes up less than half a second [00:11:00] we double from 50,000 to 100,000. And that's spread around the world, with the number of nodes being the number of members that we have, they're governing members.

Oh, but what if you were willing to settle for one continent instead of five continents? Well, if you're willing to settle for one continent like the United States, we go across the United States, more than 2,000 miles, more than 3,000 kilometers, how fast can that go at the same amount of latency? 250,000 transactions per second, a quarter million, [00:11:30] still same latency, three seconds latency, that's fast. Oh, but just for fun, what if we did one region? Okay, just for fun, with one region, 500,000.

Demetri Kofinas: How many miles is that for example between nodes?

Leemon Baird: Over 2,000 for two regions.

Demetri Kofinas: For the one region.

Leemon Baird: Oh, they're all very close to each other, just for fun. There're scenarios when you do it, certainly permission scenarios, and even the public network, but it's just to show you an idea of how this scales. And if [00:12:00] you want to know how it scales you have to read the paper, just a few numbers doesn't tell you. But the bottom line is that it would appear, if you just looked at the algorithm in the math, that we should run right at the limit, we should be able to tune it ... I mean, we haven't tuned it yet. Well, we should be able to tune it to run right at the limits of what the laws of mathematics allow, to what the speed of the internet itself allows. These results look more or less like we're in that ballpark.

Demetri Kofinas: Right there you're alluding to the way in which you arrive at consensus, which is you add a very [00:12:30] small amount of data, which is basically the metadata, the gossip about gossip to the communication, to the data that you're spreading out throughout the network and that allows the computers on the network, the nodes to run virtual voting algorithms locally on the data, which allows them to come to consensus.

Leemon Baird: You got it, that's what it is. You have to spread your information out just to get the transactions out to everybody with their time stamps and signatures, you have to do that just to have a replicated ledger, this is the only way you could do it. But then to make us do [00:13:00] everything else, we just add 1% more bytes and that's it.

Demetri Kofinas: So the performance results, I've seen these tests that you did, these were for the one to two regions, it was 128 computers, you went up to 128 nodes.

Leemon Baird: True. We have experience with that, will also publish things later that have it go up to 1,000, right now we have it up to 128, and you get slower. You got to get the paper to see all the details.

Demetri Kofinas: For sure. And audiences, people will have an opportunity to look at that, just sort of to make that point or two, when you're talking about this trade-off between throughput and latency, it's kind of like a slope [00:13:30] of about seven degrees or something like that between these two, there's a general trade-off.

Leemon Baird: Yeah, there's a trade-off.

Demetri Kofinas: But the big tradeoff is really about the number of nodes and really the distances between those. That's where you get the real trade-off in terms of having to give up give speed and sort of the number of transactions that you can process.

Leemon Baird: Exactly, there are many variables here.

Demetri Kofinas: This also doesn't take into account the processing that happens on the node level.

Leemon Baird: Let's talk about that.

Demetri Kofinas: Let's talk about that. And let's talk also about bandwidth, how do you ensure that and how do you know ... I mean different nodes will [00:14:00] access to different types of bandwidth.

Leemon Baird: Yeah.

Demetri Kofinas: Depending on where they are, and what region.

Leemon Baird: Sure. And in my cheap apartment I have a gigabit of bandwidth. Bandwidth is getting ... in some areas, is getting cheap these days. 5G cell phone you're just supposed to go to 1.5 gigabits, I'll believe when I see it. But there was recently a test by one the cell phone companies in several cities that said, 1.5 gigabits on your cell phone, so that's nice. We're actually, in these experiments we end up using, when measured it looks like we're using a small [00:14:30] fraction of a gigabit. This is one of the two things we need to do, somehow, we were not getting the full bandwidth that we were supposed to be getting and so maybe it'll get faster when we have more bandwidth.

But the bandwidth is not unreasonable, it is entirely possible that a home with an ISP will have more than enough bandwidth to run this thing. So there's that. And then the second thing is you asked about ... Wait a second, what about processing the transactions? Great, we get consensus on the order of the transactions and wonderful, we have a timestamp on each one, a consensus [00:15:00] community timestamp, the time that it'll reach the community, that's a big deal. But that's not all you need in life, you need to actually process the transaction to make them do something.

So how much time is that going to take you? Now the good news is it's purely local, something your computer does by itself. The processing is all local, the bad news is it could be really slow. It depends on the transactions. For example, what if we're doing cryptocurrency transactions? [00:15:30] Alice wants to send money to Bob, she sends ... You're a full node on our network, she sends you this transaction and says, “Please make it happen.” You send it out to everybody. You can send out lots per second, they get resolved very quickly. And now that you have consensus on it, you can apply it to the state.

What do you need to do? Well, you have to change two numbers in memory, you have to decrease Alice's balance and increase Bob's balance, because it was a money transfer, cryptocurrency [00:16:00] transfer. That doesn't take any time, changing two numbers in the memory of a computer doesn't take much time. But you have to check a digital signature.

Demetri Kofinas: And that takes time.

Leemon Baird: That takes time. That takes a lot of time. It turns out that to check one of these digital signatures is enormously computationally intensive. This is the thing that's going to take up all your time.

Demetri Kofinas: One of the things I was going to ask was if there are also GPU implementations or hardware [00:16:30] sort of modifications that you're going to expect to happen in order to sort of accommodate this. But go ahead, I didn't mean to interrupt.

Leemon Baird: Yes. So you asked about GPUs. And just to be clear, I was talking about all the time is going to be verifying signatures on these transactions, that's separate from verifying the signatures that are needed for consensus. So when I gave the speed numbers, they were including verifying signatures for consensus and they were including everything super strong encrypted, they went over the internet. We were encrypting all of our messages, we were [00:17:00] digitally signing everything, we were using secure cryptographic hashes, all that cryptography stuff for consensus was being done and it was still the speeds that I said.

But we were not verifying that signature on every single transaction, that's where all the time is going to be, because if Alice wants us to move money from her account to Bob's account, she needs to prove that she had authorized it. She needs to digitally sign that one particular transaction. So, [00:17:30] that's slow on a computer, on a typical computer, maybe a supercomputer is fast. On a typical computer that is slow, but you know what? A typical computer has a graphics card and that's what you're alluding to, a GPU, a graphics processing unit.

What if we were to verify our signatures on the GPU? Could we do it faster? GPUs are really cool. They do graphics but really what they are, are thousands of little tiny computers in one board, which is great. A normal computer chip might have four computers in it, [00:18:00] four cores or eight hyper threaded cores. These will have thousands, 1,000, 3,000, 5,000 on one board and you can have multiple boards in your computer.

Demetri Kofinas: You can use your Tesla. People are doing that right now to mine Bitcoin.

Leemon Baird: I think I've heard that. I love it.

Demetri Kofinas: It gives Elon Musk an alternative revenue stream. So go ahead, I'm sorry, I didn't mean to drop you on that.

Leemon Baird: But that is so cool. So people use these graphics cards to do these things, and they're not just using it for graphics, the big thing now is deep learning. They're using it for deep learning with the tensor units, [00:18:30] we don't need the tensor units, we need the little tiny units cores, not the tensor cores. But tensors cores are really cool too. Actually my background in that area, which is funny. But what we thought was, wouldn't it be cool to try this? And there was no software out there for it, so we had to get some software written for it, but some software is written for it.

We tried it out and the question was, could you use a GPU on a computer to verify hundreds of thousands of transactions [00:19:00] per second? And the answer turned out to be no. The speed is not hundreds of thousands, it's a million. Literally was 1.18 million verifications per second, and that's not peak. That's not just to do one batch, that's continuous. Every second we were doing 1.1 million and the next second, we're doing another 1.1 million and just continued. Okay, that's overkill. We can't even get consensus on that many transactions per second which means [00:19:30] that it looks like it shouldn't be fast. That's the answer.

Now if you can run a smart contract that takes a year to run, then of course you're not running that fast. And all the devil's in the details and you have to look at all the details or read the paper and look at what's happening. But the bottom line is that as far as we can see right now with our experiments, it looks like the system is going to be fast.

Demetri Kofinas: And we can get into ... I mean I think it'll also give some clarity to people if they can [00:20:00] wrap their head around some of the implementations or some of the possible use cases. Before we do that, I want to ... You talked a bit about consensus time stamping, that's super important and it's something that we've covered in our prior conversations but I think we haven't covered it enough and I think now is where it's particularly relevant, because I think it's one of the most unique, if not the most unique thing along with your consensus that Hashgraph offers, which is this fairness of ordering transaction.

Something that you can't do [00:20:30] on a block chain, because you have a leader that is sort of assembling the transaction within a block. Can you explain how fairness works with Hedera and Hashgraph, and how that's different than the alternatives that exist currently in the market, and why that's so important?

Leemon Baird: Yes. So Hedera and Hashgraph, how do we do fairness? What is fairness and why does that matter? By the way, we haven't actually talked about Hedera and Hashgraph. Are they the same thing? Two different things? Let me explain. [00:21:00] Hashgraph is the algorithm, the math and the computer code that makes us all come to consensus. You could use that for a bunch of friends in a permission network or a bunch of competitors in a single industry in a permission network or you could use it in this big public network named Hedera. So Hashgraph is the technology that Hedera uses to provide the planet with a public ledger.

Demetri Kofinas: It's the bottom layer of the stack.

Leemon Baird: The bottom layer the stack. And Hedera is the whole stack that we're building, and then [00:21:30] the whole world will build layers on top.

Demetri Kofinas: And if you want to think about this in terms of the entire sort of all the software, the consensus protocol sits on top of the internet protocols that enable the communication.

Leemon Baird: That's it.

Demetri Kofinas: So this is all one giant stack for everything including consensus.

Leemon Baird: You've got it, exactly right. So at the bottom you've got wires and fiber optic cables and microwaves and satellites around the world talking to each other. Above that you have TCPIP, standard internet protocol stuff. IPV4 and IPV6, we support both and we support [00:22:00] firewall piercing. We support all sorts of things. Above that you have TLS, we want to encrypt it, we want to make sure you're getting the right stuff and we have that, CLS 1.2 using CNSA compliant key sizes and algorithms, which means the US government, that you protect top secret with it. It's that strong.

Bigger key sizes, we're actually doing more crypto work here than most systems do, you could say it's overkill. I think in some ways it is overkill but we want it to be compliant with the standard. We're trying to do things right. So at that layer we have TLS, [00:22:30] above that Hashgraph. Hashgraph makes us gossip to each other, makes us time to consensus on the order and on the timestamps, which you asked about, which we'll get to in a second. Above that, we've got the services, we have a file system, we have a cryptocurrency, we have the smart contracts and then above that you have everything else.

All the distributed apps that people are building on their computers or in their smart contracts. Those are the layers of the stack that we're talking about, and I just said at the top you have everything [00:23:00] else, you can even view that as a whole bunch of layers.

Demetri Kofinas: And get to be built layers really because that's ... You're building a platform on which you're hoping to attract developers and building people that are going to develop incredible applications that are going to run, that are going to be the use case solutions.

Leemon Baird: Yes. So a whole bunch of layers we hope to be built someday. Right now the biggest community would be solidity developers, there is an enormous ecosystem of solidity smart contracts out there, worked, debugged [00:23:30] in use today, all of it runs on us on day one.

Demetri Kofinas: So you're able to port over all these applications that have been built for other platforms and you're going to be able to run it on Hedera.

Leemon Baird: Yes.

Demetri Kofinas: That's pretty remarkable.

Leemon Baird: Without change, yes. So that's a good first step. The first step is we're taking ... the entire universe actually runs on top of us, but that's the first step, it's not the whole universe. But solidity is actually a pretty big chunk of the universe.

Demetri Kofinas: Well, it's Ethereum. Is there anyone else that uses solidity?

Leemon Baird: [00:24:00] Well, yeah. I don't even know everything that everyone is using and there's a number of different languages and you can even do things in different ways. There's bytecode versus the source code. Let's not get into all of that.

Demetri Kofinas: Sure.

Leemon Baird: It's a large ecosystem but if you had to pick one thing to be the most common, I would say solidity and we support it without any changes right of the box. All those solidity libraries that are out there all run unchanged on top of us.

Demetri Kofinas: I mean the reason that you did that obviously seems pretty obvious and that's simply, you want to be able to make this [00:24:30] as user friendly as possible, and the fact that there have been so many people that have poured tremendous amounts of money and time and resources into building these applications that could run on distributed Ledger technology, the fact that you're making it easier for them to do that on Hedera makes obviously a tremendous amount of sense.

Leemon Baird: Exactly. That's exactly it. And we actually have some ideas about smart contracts, and we may come up with this separate smart contract system that will also support that has better features, but for right now, obviously the best way ... You said the top layers are yet to come. But the best [00:25:00] thing to do is to start with the top layers not yet to come, have the current ones work and then people can build other top layers.

Demetri Kofinas: So we're going to bounce around now, because I had this whole idea in my head about how I wanted to do this, but you know what? Let's get right to this, because we're talking about solidity, we're talking about smart contracts. Let's talk about what you and I have spoken about which is what you think will be the killer app of this platform, which is micro-transactions, basically the cryptocurrency.

Leemon Baird: And let me be clear, killer app as of day.

Demetri Kofinas: As of day one. Please explain this because this is really exciting.

Leemon Baird: Yes. [00:25:30] So I think that everyone says that ledgers are going to change the world and they're right. In the long term, ledgers will affect everything that we do, the whole planet does. In the short term the killer app for something like Hedera, has got to be theses micro transactions, nano transactions.

Demetri Kofinas: What is a micro transaction? What is a nano transaction? Explain that for viewers that may be unclear on that.

Leemon Baird: Sure. And I just made up nano transaction on the spot. But we're talking about is, you want to be able to have everyone have these cryptocurrency [00:26:00] accounts that hold cryptocurrency, and you want them to be able to move money between accounts, going to be able to buy and sell things. And if I have to pay a

dollar a transaction, there are useful things I can do in the world. If I have to make a big purchase, I don't mind adding a dollar as a transaction fee, but you know what? I'm not at that point, going to pay a tenth of a cent to you to listen to a song once on a streaming music station.

I'm not going to pay a dollar of transaction fee to pay you [00:26:30] a tenth of a cent. If I want to really have small transactions, then we have to have low transaction fees. But if I'm going to have low transaction fees, then it has to be cheap to run a full node per transaction, which means first of all, it has to be cheap to run a full node not a mining rig. I can't have a stack of those Titan boards that you're talking about or ASIC boards which are even more expensive. I can't use tons of electricity, so proof of work becomes problematic. [00:27:00] I have to have a cheap computer, I have to be able to use ... Well, my cell phone has enough power.

In fact, you know how we test our network? We often test it on his network of Raspberry Pis. Raspberry Pi is a little $30 computer. That's what we often use as one of our full nodes, one of our miners, because it doesn't do mining, it's not a miner, it's a full node. So you have to have it cheap, but also there's some cost involved, you have to amortize it over lots of transactions, so you need to have very high transaction throughput. If you can be doing hundreds of thousands of [00:27:30] transactions, and you don't have to do proof of work, and ordinary computer can run this on the kind of bandwidth it's available in an apartment.

Then you can talk about having very cheap transaction fees, which in turn allows you to do whole new kinds of transactions in the world, and so you can talk about a world where maybe instead of playing games and going to websites and watching videos where you're paying for [00:28:00] by watching ads, you pay for it by paying one hundredth of a penny. Does that matter? Well, guess what comes along with paying for it by watching ads? Whoever is showing you the ad, has a very strong motivation to spy on you, that's just inherent. People have said, “You know if you're not paying for this service, you're not the customer, you're the product."

Demetri Kofinas: When do you expect ... Let's sort of just around this very specific thing of micro transactions, [00:28:30] what are we talking about let's say a year out, a year from now? Will I be able to pay for my Starbucks coffee using Hedera? Will people in Africa or the Middle East or in Asia be able to use this platform to actually conduct what are the equivalent of cash transactions for the first time? Because obviously that was the hope with Bitcoin but because the cost is so high because of proof of work, and we're going to get also into proxy staking, I want to get into proof of stake, [00:29:00] which is how you protect the network. But what are we talking about here in terms of in the year’s time?

Leemon Baird: Exactly. So who knows how fast things will roll out? But things are just making my head spin how fast they're rolling out right now. South by Southwest is going on as we are recording this interview and I assume at some your viewers will see what was announced at South By Southwest in using this for micro payments in the creative industry. You talked about peer [00:29:30] to peer payments, how do I send money to somebody using my phone? It turns out there are countries where this is very

common, but it's very commonly run by one central server controlled by one single company that controls the whole thing.

Maybe you'd like some more trust, maybe it'll be nice to have a distributed system. But you're not going to do it if you have a dollar fee. Well, maybe you would but maybe you wouldn't. Maybe I don't want to pay a dollar every time I give you a couple bucks through my phone, but if you have a hundredth of a penny fee or some other fraction of a cent, I don't know the prices right now. [00:30:00] But if you have a small fee, maybe it makes it easier to send money back and forth. And then maybe when people are used to that, you do pay your bus fare when you get on the bus with your phone, which by the way some countries have had for many, many years, not ours.

Maybe we'll catch up to the rest of the world of technology some day and be able to pay for your coffee at Starbucks using your phone, using a system that's more trustworthy than a central server. So this is where we're headed with these micro transactions, they allow us to move to an economy where maybe there's not so [00:30:30] much spying on you because there's not the adware and maybe there's new things we're paying instead ... Maybe instead of listening to a streaming music service where you have to pay them $10 a month, you're just paying a tiny fraction of a cent per song. Why is-

Demetri Kofinas: Because the transaction costs are so low.

Leemon Baird: Exactly.

Demetri Kofinas: And the fees aren't there.

Leemon Baird: And why is that better? Because then I could listen to multiple services. I can switch back and forth, I don't have to pay each of them $10 a month, I just switch back and forth.

Demetri Kofinas: Yeah. It's gives you power.

Leemon Baird: [00:31:00] Yeah.

Demetri Kofinas: It opens up an entirely new world of what's possible, we've been imagining this world for years because we've all been thinking about and sort of wondering what would it look like, what can we build. Many people have spoken at length about what a distributed future could look like, but what we're talking about here is actually that we might actually be there, [crosstalk 00:31:19] Hedera. I mean this is really what you're releasing. Let's talk a little bit further and get into a little bit more detail about how it is that you make it possible to keep those fees low, because [00:31:30] proof of stake is sort of the alternative to proof of work that some of these other systems are trying to go to. of course, because of the way that you reach consensus, you're able to use stake in order to secure the network in a way that allows you to keep fees low where it's still secure.

Leemon Baird: Yes.

Demetri Kofinas: Can you explain how proxy staking works the way you guys do staking and how that all integrates into this conversation?

Leemon Baird: Absolutely. So yes, we do proof of stake, there are other systems that are called proof of stake, they do proof of [00:32:00] but they also underneath it have a simulated economy or some other system. It's similar to the confusion about DAGs. People talk about DAG technology. Well we use DAGs, they use DAGS, but they are radically different technologies, they don't really have a lot in common. So these terminologies are all very confusing. But here is what we are doing, we have a system that is Asynchronous Byzantine Fault Tolerant.

This is something you don't see in some of the systems that you're referring to, they are not Asynchronous Byzantine [00:32:30] Fault Tolerant, which causes some problems. It's possible that a malicious firewall might be able to cause double spending to happen, it's possible that a pretty small bot net of compromised computers might shut down one computer at a time and shut down the whole network. This future we're talking about, you can't afford the global economy to shut down for a few hours because there's an attack.

Demetri Kofinas: Just to be clear there for our listeners that are listening, what you're alluding to the first case, the fact that some of these alternative like a block chain network forks, and then the fact that there's a leader that's chosen to put the block [00:33:00] there, which is why you can DDOS that as opposed to Hashgraph. I'm I correct?

Leemon Baird: What you're saying is almost right, so what we're talking about in the proof of work systems there may be vulnerabilities to a firewall that divides the network into two halves, and then each half starts building its own block chain, that's a problem. You could say, "Oh, I'll do firewall detectors, I'll just detect one half of a shutdown." But what if we also have a bunch of malicious nodes that can talk through the firewall? That's also a problem. They also have problems with consolidation. If [00:33:30] everybody lives in one country, you have a problem.

But the other problem is with leaders, there you have the problem that if somebody is a leader then a bunch of compromised computers can flood them, shut them down and it shuts down the whole network. And here's the real problem, you may have leaders and not even understand that it's leaders, the system doesn't sound like its leaders. Maybe it's delegated proof of stake, where there's no leader we just have a couple dozen people that take turns acting as a leader for two seconds. [00:34:00] Guess what? That's a leader, because you know what the bad guys can do? They can take their compromised computers, flood the current leader for the whole two seconds that they're a leader, and so when someone new becomes leader guess what they do?

Demetri Kofinas: Follow the leader. Follow the leader. We don't have a problem.

Leemon Baird: So I can continue to answer your question but go ahead and ask the new question.

Demetri Kofinas: This is the thing, I spent some time going through the white paper and this particular example, we've talked about this before about follow the leader. And I was trying to [00:34:30] think about theoretical attacks against a proxy stake system, as if I'm someone that would be able to come up with these attacks. But I had some fun doing it and I came to this one, and I'm going to just wing it here and throw it out there which was follow the fat node, and I'm just thinking since ... And you can explain how proxy staking works and maybe you should first before I start going into this but my question is, are there ways that you might potentially be able to compromise a proof of stakes system the way you guys have done it.

If there are certain [00:35:00] nodes that are overly weighted, because your votes are weighted according to your stake. If you have a large stake is it possible for a virus to be sort of in the network and sniffing out which are the biggest nodes, following them into their shards and basically attacking those shards on a regular basis or attacking where those nodes are? Does that make any sense?

Leemon Baird: Yeah. The short answer is we don't let that happen.

Demetri Kofinas: Okay.

Leemon Baird: So we balance the nodes. And the longer answer is, well of course any proof of stake system would have that issue, which is the whole point [00:35:30] of making stake be well distributed, which is the whole thing that drove this structure of our governance and our release schedule and of our staking system and of our proxy staking system in the first place.

Demetri Kofinas: So these are all by the way.

Leemon Baird: It's the central purpose of it.

Demetri Kofinas: And these are all things that people will have to learn about and read independently and everything else, so they cannot learn about everything here, I'm trying to find some way to do that but please continue.

Leemon Baird: Great, so I think we have a stack now of three questions that are in the middle of answering right now and I am remembering them but at some point, my stack overflow, which is fun. [00:36:00] This is all just fun, we're just hanging out and talking. But I will talk about the proxy staking and staking in a second, because it's a large subject. But you get asked, how can we be cheap? And I started saying, we're cheap because we don't have leaders. That's right, I was explaining some terminology. But we don't have leaders which is not a bottleneck and we don't have proof of work which is expensive.

If you don't have the leader to slow you down, because the leader has to talk to everyone so everything flows through the leader, and if you don't have [00:36:30] proof of work, which makes you buy a supercomputer and use lots of electricity, then you can have very high speed and very low cost to the computer involved. And that's the combination you need for

low transaction fees. Also, just to be clear we have to not ignore the laws of economics. There are systems that say, “Well everything's free.” There is no such thing as a free lunch in the long term, in the short term there is, in the long term [00:37:00] there isn't. You have to make sure that ultimately the fees you're being charged balance out the cost of the network to provide the service, because ultimately there's a limit to how much charity the node runners are willing to do in order to give you a free service.

If it costs them actual money to run their node and they're not getting actual money that equals that, then eventually they'll stop running nodes which causes consolidation to fewer nodes, which undermines security, the whole point of this system.

Demetri Kofinas: So you don't expect to see economies of [00:37:30] scale on the nodes?

Leemon Baird: Short answer no, which is great. Longer answer, economies of scale can happen but it doesn't hurt us for the following reason, because to answer your question which almost depletes the stack of questions you've asked.

Demetri Kofinas: Good.

Leemon Baird: That were in the middle of at the moment.

Demetri Kofinas: So we can get to another one.

Leemon Baird: Yeah, we only have fairness now in stock I think. But your question is, how does the staking and proxy staking and that stuff work in order to stop Sybil attacks, when the whole purpose [00:38:00] of it is to stop Sybil attacks. All systems can be destroyed if the bad guys are controlling one third of the influence, which is one third of the nodes if every node gets a vote, one third of the stake if every coin gets a node. One third of the hashing power if each hash per second gets a vote. You understand I'm saying. Whatever is influencing the system, if the bad guys get a third of it, you're dead, assuming they also have firewalls. So [00:38:30] everything we have done in the structure of Hedera is starting from the point of, let's make everything distributed. The important thing about distributed ledgers is that they be distributed.

Demetri Kofinas: Kind of integral.

Leemon Baird: Kind of integral. You sort of have to do that. There are major ledgers, block chains where half the hashing power is controlled by three or four people. Okay, it is distributed to [00:39:00] three or four people.

Demetri Kofinas: And that's a result of the economies of scale that exist with proof of work specifically.

Leemon Baird: That's a problem. Economies of scale and also you have to use a scarce resource that's cheaper in some countries than other, electricity. Both of those cause problems.

Demetri Kofinas: Which is why we seen these huge mining tools in China for example.

Leemon Baird: Right. So all those sorts of things and it's what you'd expect. What you need to do is have it be so cheap that we can end up with millions of nodes spread kind of uniformly around the world. Similarly, with the coins, we need to make sure that the cryptocurrency [00:39:30] is uniformly spread out or you don't have whales that own it all. One whale that owns it all, destroys your system and so we have a very slow schedule for how we release it into the market and we're taking steps to make sure it's widely distributed and initially it's held by the 39 not by one, but by 39 so they act as a check on each other.

Demetri Kofinas: That's the council, the governing council.

Leemon Baird: This is the council. This is the Hedera governing council, yes. The hedera Hashgraph council is a council of 39 members and they're large and no one of them can control a third of [00:40:00] it, because each one of them only controls a thirty-ninth of it. That's the whole point.

Demetri Kofinas: These international corporations, organizations.

Leemon Baird: Absolutely. Big, well known, competing with each other and it would take ... Even if a dozen of them collude were fine, you have to take 13 of them to collude to cause a problem. And it would hurt the reputation because remember the transparency thing we talked about, everything is transparent. If they slip something nefarious into the code, everyone on the earth will know it, because a million nodes [00:40:30] have it and a million nodes see the source code and recompile it and compare it in node. So the very first thing we're doing is ensuring that these coins are evenly spread among the coin holders.

Furthermore, there's a limit to how many coins one computer can stand up and so you don't have a network or a shard where one computer has all the coins and all the other ones are little, because again in your shard, if one computer has a third of the coins it can destroy the whole shard which stores the whole network. Our security comes down for [00:41:00] making sure no one third ever controls, so we assign people to shards to make them fairly uniform in how many coins they have, we have a limit on how much coins you can have in a given computer. If you happen to have a huge number of coins, you're going to have to stand up a large number of computers.

There is where a little bit of economy of scale can come in, which is great. It just makes things cheaper for everybody. I love that, but you can't put all of your coins on one computer, you actually have to help the network and we will end [00:41:30] up randomly distributing your computers to different shards and we haven't talked about sharding yet but it's critical to security to make sure that we do this right, which almost brings us back

to your second question that's unanswered, which is how does staking and proxy staking work? What is that? If you would like, I want to answer that.

Demetri Kofinas: I would love it.

Leemon Baird: Let's talk about that.

Demetri Kofinas: Let's do it.

Leemon Baird: Okay, the whole problem comes down to, if a third of the influence is controlled [00:42:00] by bad people or if a third of the influence is by people who just go to sleep and don't do anything, that's bad, in another sense, then the whole system freezes or is compromised. If they're malicious then the whole system is compromised in a malicious way, and if they just went to sleep then the whole system goes to sleep.

Demetri Kofinas: You're saying that they don't stake their coins. Is that what you're talking about? What's the analogy here for sleep?

Leemon Baird: True. Yes, they don't stake their coins, or if we're counting by nodes if they turn the computers off, or if we're doing that [00:42:30] by hash power, if they turn their hashing rigs off. Their mining rigs off.

Demetri Kofinas: There's a revolt.

Leemon Baird: There's a revolt. So if a third of us don't do what they're supposed to be doing then we have problems. If a third of us do something malicious, then we have problems. How do you deal with that? Well, first of all we have to decide how we're going to give influence. Is it going to be by mining rigs and how much electricity you're willing to buy? And I want to go down that route because I don't want people to have to buy lots of electricity and use money rigs. Also, that causes consolidation due to economies [00:43:00] of scale because it's cheaper to buy the big boards or cheaper to buy the basics the ASICS, you move to countries, you have geographic concentration, I don't go that route.

So how about voting by computer? Problem, one person might stand up a whole lot of computers, there's an enormous economy of scale there, that's a Sybil attack or somebody might have a bot net where they've compromised a whole bunch of little computers, like the computer in your printer might have been hacked into over the internet. It becomes a full node; one person now controls a third of the full nodes out of luck. We have to avoid that. [00:43:30] How do you avoid that? Well, the third option is your influence comes from the coins you have. How much cryptocurrency do you have? I like that, because it's a scarce resource, nobody can Sybil attack lots of coins out of nowhere, that's the whole point of a cryptocurrency, is that it's a scarce resource.

Also, if the cryptocurrency becomes of value, you use it to actually do things in the ledger. Everybody wants it because you can actually do things. [00:44:00] You use cryptocurrency to store files and to retrieve files and to run smart contracts and to move cryptocurrency.

Demetri Kofinas: It's like fuel.

Leemon Baird: It's the fuel of the whole system. It has an intrinsic value, it is a utility. In fact, the term utility token is often used. There is utility to this thing, you need usefulness to this thing. Then it's hard to corner the market, for the same reason it'll be hard to corner the market in real estate. You probably couldn't go out and buy a third of the real estate in United States.

Demetri Kofinas: If your market cap is large enough, [00:44:30] right? [crosstalk 00:44:30]. That goes back to the governance and the release of coins and the fact that you have to care how big your market cap is.

Leemon Baird: Exactly.

Demetri Kofinas: The bigger your market cap in a proof of stake system, the more secure your network.

Leemon Baird: You've got it. And also, if you have good fluid markets then anyone who starts to try to corner the market, guess what the market notices, "Hey, somebody is buying massive amounts," and guess what the price does, it goes up, which makes it harder to corner the market. Markets are self-correcting in that way as well. So these are things that we are dealing with. I [00:45:00] like the idea of letting your influence be proportional to the cryptocurrency. It makes a lot of sense. And I'm not the only one saying this, pretty much everybody is saying this, good answer.

Okay. Now some people also go further and use the cryptocurrency to in some sense drive the consensus itself, it's economic self-interest that causes you to choose what algorithm to run and use game theory and economic theory and there's real problems with that, and none of those are Asynchronous Byzantine Fault Tolerant ever have [00:45:30] been proven, doubt they ever will, it's too complex. It's like proving the US stock market will never crash again, no one has proven that, you're never going to prove that, it's not true.

Demetri Kofinas: Well, that's an interesting point also too. And just generally speaking with proof of stake, the fact that there're ... and with tokenized software in general, there are these economic forces and market forces that are sort of in the software that are ... It's actually kind of cool, the fact that you're engineering something with these types of variables at play, this level of complexity. It's got to be a lot of fun doing it.

Leemon Baird: It is. Crypto [00:46:00] economics is fascinating, it's really fun to be playing in this field. And the bottom line is, we have to not ignore real world economics. And if real world economics says the security of your system depends on the stock market never crashing, then you do not have a secure system. But if it says, "You know, if it's cheap to run a node and you get paid to run a note," I'll bet lots of people will run nodes. That does recognize real world economics or if real world economics says, "Once we have a well-functioning cryptocurrency [00:46:30] with actually utility, a utility token, then it becomes

hard to corner the market and we're going to stake our security, we're going to base our security on it being hard to get it through the coins," that's really good.

Okay, oddly enough I'm not going to say this, lots of people have just said that. That proof of stake is a good way to balance your influence. And they've also said it's a good way to do your consensus which is a bad idea. But it's also a good way to base your influence. So for us we have this virtual voting system, it goes back to 30 year old algorithms, [00:47:00] we're using voting, it's virtual voting. We weight the vote by cryptocurrency and that ensures we are secure as long as you don't have a third of the people failing to use their cryptocurrency or starting to do something malicious.

However, I just slipped in a word there. I said we are in trouble if a third of the people aren't using their coins. I said that a full node [00:47:30] that is part of our network, that is doing the voting, the virtual voting has its votes proportional to the coins that it's holding. But what if all of our full nodes together aren't holding all the coins?

Demetri Kofinas: Just to sort of clarify your point, it may not be something I want to do. I may own some coins but it's not really something that I'm looking to do to run my computer to participate in validating the ledger.

Leemon Baird: Exactly. Seriously, we would envision that eventually there would be millions of full nodes, the [00:48:00] billions of cryptocurrency holders. So that's .1% of the market or a little fraction of .1% of the market of the coins maybe are being held by full node runners, but then that's a bad thing, because you don't have to corner a third of the coins, you have to corner a third of .1% of the coins, that's a disaster. So we have proxy staking. Here's what proxy taking is. You might want to run a full node because [00:48:30] we're going to pay you to run a full node, that's really nice. Once a day you get money based on how many coins you had and the fact that you were participating in more than 90% of the rounds or some such threshold.

Demetri Kofinas: It's like interest earned on deposit.

Leemon Baird: Haven't got to that part yet. It's like being paid for your work, for doing your job.

Demetri Kofinas: Got it.

Leemon Baird: If you are a taxi driver you're paid per mile that you're driving or at least you're paid for driving. Let's not say that, it's more like a bus driver, it's not per mile. It's just you have a salary and your salary is because you're doing the work. [00:49:00] We're not like a taxi driver, we're like a bus driver. You're paid for running the node and for running it throughout the day and participating 90% of the rounds. And you're paid proportional to how many coins you have, that's why you'd want to run a node. But most people are not going to run a node, I want cryptocurrency because I want to use the services. I want to be able to store files and I want to read files and I want to be able to run smart contracts, I want to move money back and forth and I want to be able to buy a coffee

at Starbucks. I want to [00:49:30] use it for cryptocurrency purposes, I do not want to run a node, and I'll be in the majority.

So what about all that money that's sitting in my account, that isn't being used in nodes? That would be a disaster. So we would do exactly what you just said, it's called proxy staking. I would pick one of those million nodes that are running out there and say, “Hello node, I am willing to let you get credit for my coins.” Remember [00:50:00] how it gets paid proportional to how many coins it has, well has can include my coins. What we're doing is paying it according to how many coins it stakes, but it can stake the coins it owns and maybe if I'm nice to it, it can stake the coins that I own. It can stake them as a proxy for me. I am proxy staking to the full node. Well if I'm proxy staking to a full node, then that full node now is making more money, so it wants me to proxy stake to it.

And we can agree to split [00:50:30] those fees, it gets money paid to it proportional to its own ownings, and gets the whole amount. It also gets a fraction of what it gets based on my coins and I get a fraction of what it's based on my coins, and we can even have a market where we negotiate who gets what fraction. And so I might pick one of those million nodes and say, “I'll give you half of my earnings or 10% or 90%.” I don't know, we'll work out something. There'll be [00:51:00] a free market in that.

Demetri Kofinas: Sort of in your white paper there are three types of fees. There's node fee transaction fee and services fee, that's the ...

Leemon Baird: Plus payments.

Demetri Kofinas: Plus payment.

Leemon Baird: Payments is this, the payments for being a full node is the fourth thing, plus is the three fees. Let's put that on stack and get to that in a second. So the proxy staking is that we're going to have this market where you can choose a full node to send your money, not send your money. Let's be really clear, there's no bonding in this system, for [00:51:30] the nodes or for the proxy stakers. You can say, “I proxy staked to that node, and I've decided to give a 37.2% of my earnings, that's what we've negotiated until the nano second that I decide to stop this. And any moment I can send my money somewhere else so I can change how I'm proxy staking, the node has no say in that."

Demetri Kofinas: Because some of these other alternatives have bonded here.

Leemon Baird: It's a fair analogy the bond is like a CD account, like a time deposit versus a checking account and a non-bonded where you can [00:52:00] withdraw any point without penalty.

Demetri Kofinas: Yes.

Leemon Baird: In both cases ... Yeah. We have a checking account not a CD. you've got it. So the bonded systems would force you to say, "Well, leave it there for a month," or

whatever. We don't do that. The full node itself also gets paid according to its own money, its own cryptocurrency but at any moment, it can transfer out as much as it wants. It just stops getting money, just like an interest bearing checking account would be the same way. You can send the money out anytime you want, you can write a [00:52:30] check and you earn interest up to the time when you send your money out, very free. Also, some of those bonding systems have penalty fine systems as well, you actually lose money if you do wrong things.

Demetri Kofinas: Right, you're penalized. There's actually a name for this, slashing I think. Something like that but ... Correct, yes.

Leemon Baird: Yes, we don't have that. If you're a full node, you know how much money you're risking? Zero. Zero [00:53:00] risk of your money. As long as you leave the money there, and hold the money and stake it, you get paid for it. It's like earning interest to your checking account, and as soon as you move away you stop earning interest, but nobody will ever fine you for that money. We'll talk about transaction fees in a second, but those are safe and I'll explain that too if you're interested, get really in the weeds.

Demetri Kofinas: Yeah for sure. I want to get in the weeds here Leemon. This is why we're here, we're here to get in the weeds.

Leemon Baird: I love it. I love weeds. Weeds are math and math is fun.

Demetri Kofinas: Yeah. Well, this is exciting because [00:53:30] you have real problems to solve. I mean this is really cool. Anyway, I keep interrupting please go ahead.

Leemon Baird: Oh, but it's great, your interruptions are great. So you had the full node that's staking, you had the node that is proxy staking to the full node, the proxy staker at any moment can change who they're proxy staking to and it's in an account that they can spend money from any moment, you just start earning less interest when you do so. So it's all good, and if you have a choice between proxy staking and not proxy staking, why not proxy stake? You get money. "Oh, but that'll be inconvenient, right?" [00:54:00] No, here's the deal. You are probably as a consumer using things the easiest way you can, you're going to have a wallet program on your phone or on your laptop that tells you how much money you have, keeps track of your cryptocurrency, allows you to send cryptocurrency to other people.

It's part of the process when you buy things with the cryptocurrency, it manages it all. It was written by somebody, Hedera is writing this one, it's actually nice, it's on my phone, it's pretty good software, [00:54:30] I like it. And our plan is to encourage everyone else to steal our source code, we're giving that away. Steal our source code, build better ones and put us out of business of distributing wallets. But for the moment we're distributing wallets to jumpstart the system, and guess what? I predict every wallet person in the world will ever do, anyone who writes wallet software will do, they will give you an option to proxy stake or not. By default, do you think they'll have it on or off?

And do you think it [00:55:00] will proxy stake to the person who wrote the wallet or not? Obviously, the person who writes the wallet software will get money if everybody has a default of proxy staking to them. And I expect a big ecosystem of different people writing such software, which means a thriving distributed market of who's been a proxy staked to. And all the coins will [crosstalk 00:55:24].

Demetri Kofinas: That's really cool. Also, just generally speaking you're going to be disrupting the wallet space in general, the software industry for wallets, I mean in the [00:55:30] sense that ...

Leemon Baird: Maybe not.

Demetri Kofinas: Well, what I mean is ... Let me correct myself to make sure that what I'm saying ... what I want to say, which is that right now wallets as I understand it, the way that they work is they run on servers. People basically have their coins in sort of central areas where they can be attacked and stolen, which is why even today I forget the number, some millions of dollar's worth of Bitcoin was stolen. What we're talking about here is something totally different.

Leemon Baird: [00:56:00] Yes. So the word wallet is used both ways as well. You can run them on software that is on your phone and only you have the keys, that makes it hard for people to steal. You could also just talk to Joe's wallet server service and say, "Here Joe, here's all of my money, please hold it for me. I'll trust you not to steal it." There might be problems with this business model. I don't know.

Demetri Kofinas: And the reason why I'm saying that also Leemon is because we were talking about micro transactions before, the point is that we're talking [00:56:30] about a system with Hedera where you're going to able to conduct a huge number of transaction which is currently not possible, which is why the security concerns sort of manifest in some of these other systems because, for ease of use people end up giving up security and in terms of giving up security, you end up Mt. Gox, you end up having these other exchanges or wallets or whatever they get hacked.

Leemon Baird: Yes. You're exactly right. So does that mean all these companies got a business? No, in fact [00:57:00] I think we're going drive more business to them. That's why I say we're not disruptive. It's okay, we're disruptive but not in a bad way.

Demetri Kofinas: The positive way.

Leemon Baird: The positive sense.

Demetri Kofinas: The positive sense.

Leemon Baird: But in the positive sense of helping the car makers and putting the buggy manufacturers out of business, it's in the sense of making them money too. Here's the idea. I think that is a very bad idea for you to give some server your secret key or

private key, I don't think that's a good idea. I think what you should do is keep your own private key. There are reasons why you could still have problems, someone could hack into your [00:57:30] computer and get it but I think that it's generally a good idea for you to keep it. Then the only problem is, "But what if my computer gets erased? All my money in the whole universe gets frozen forever, I'll never get it back." That sounds bad.

So is it possible for these servers that are no longer holding your money to do something of use for you? Oh, sure. Well, they can hold your private key for you and that way if you ever lose it, you can get it back from them. Oh, but wait, we just got back to the original problem. Oh but wait, they just [00:58:00] are holding it, they don't have to use it. There's this thing called secret sharing in the world of cryptography, goes back decades, which is a way of basically taking your key and splitting it between multiple servers, where they all have to get together to recover your key. And if you trust that at least some of them are honest, then you're safe. But if you erase your wallet, you erase your phone and you have to recover it, you go to all of them and you get it back.

There's even these things called threshold schemes for secret sharing, which says, "I give it to 100 services [00:58:30] and any 47 of them can get together and recover it," or whatever you pick your numbers or 10, maybe six out of 10 are needed or maybe don't even use services, maybe I have 10 friends and family I give it to, and any six of my friends and family can get together to recover my key. We can start going to a world where we have real security without trusting any one person, you just trusted a group of people, don't have too many bad ones. Does that sound familiar? Yeah, that's the whole point of ledgers.

Demetri Kofinas: Yeah, that's distributed.

Leemon Baird: And so we take the distributed Ledger idea and [00:59:00] you apply to the wallets themselves. Oddly enough I'm not the only one to have said this, this is the way the world has to go, and this is the way that I expect it will go. The good news for the security of our system for that is that I believe everyone is going to be storing their money ultimately in their phone or in their laptop or in hardware tokens, that's a really cool thing too, we can talk about that. But Hedera doesn't care, we're agnostic but hardware tokens have a lot to be said for them assuming they have a display screen on them. [00:59:30] We can get into that.

That has nothing to do with Hedera though. But I think if that's the case, then all these people are going to end up proxy staking. Basically everyone will. Why not? It's free money, it's turned on by default, you're going to proxy stake, the fear that a third of the coins will just not be a proxy staked has gone away. And we have to make sure no one corners the market on proxy taking, but they won't, because there's going to be so many different competing wallets, that will all be proxy staking [01:00:00] in different places.

Demetri Kofinas: That adds value to the currency, the fact that you are able to proxy stake obviously, because you're able to earn interest on your ... I also have a question generally speaking about that which is hoarding. There is a propensity we certainly see that in some other crypto currencies where the hoarding, the value of the currency actually

ironically become so valuable that no one ends up using it. How do you imagine that's going to manifest with Hedera? And also, another moment to make the point that, this is not like you're releasing this code out in the wild and you're going to step away and it's going to be there for [01:00:30] the rest of time.

This isn't like that satellite they sent out to space in like the 70s or whatever, you're going to be able to make tweaks and updates as you move along. But like this is an interesting thing, the market dynamics. Could you foresee for example the cryptocurrency just becoming so valuable that everyone just perpetuating this expectation that it's going to be deflationary and they just pile into it and for a long period of time there's nothing that sort of happening in terms of transactions or use?

Leemon Baird: [01:01:00] I wouldn't vision that in the long run this becomes very much a system that people are using. This cryptocurrency is not intended to only be for store of value or hoarding. It is intended to actually be used to do utility things on this ledger and then maybe for the secondary markets if you buy everything in the universe with it and you buy a cup of coffee with it, if that is the case then they'll be people hoarding, who cares? They make up a small amount of money, [01:01:30] I don't care. Also, from a security point of view, even if only hoarding was going on, I wouldn't care as long as it's not one person doing the hoarding but different people doing the hoarding, it doesn't have any problems. You said people hoard because it's valuable, I would say they hoard because it's valuable and well there's nothing else to do with it. We're also going to do with this cryptocurrency.

Demetri Kofinas: That's a good point.

Leemon Baird: What we're going to do is say, "You can hoard it because it's valuable but there is something else to do with it." In fact, the whole point of the cryptocurrency is actually something else you do with it. [01:02:00] Revolutionary thought I know, but to actually use it as a utility token, to actually be using it as a cryptocurrency is the point of the cryptocurrency. This is the way we want it in the future.

Demetri Kofinas: I also bring it up because I did an episode where we discussed the equation of exchange and some work that Chris Burniske has done with velocity and how that would affect the value of the token and I was thinking about it also in that regard in terms of that trade-off between the utility [01:02:30] and also it actually having value as a store of value. In the interest of time Leemon, there is one thing I definitely want to get to which is your sharding implementation, which is really exciting and it's really relevant especially to any developer who's sort of wondering how are you able to execute smart contracts across shards? How are shards able to communicate with each other? How is consensus done between shards? Can you explain a little bit about how that works? I think there are some aspects that are unique to your solution. [01:03:00] Walk us through that a little bit.

Leemon Baird: Absolutely. So sharding is key here, so is fairness which is the only thing left on a stack of questions you've asked so far that we will get back to. But sharding

is important and it all comes down to the math, we want Asynchronous Byzantine Fault Tolerance. I keep saying that, but it matters. And when you do sharding it matters squared, it matters to the nth degree, it really matters. So here's the idea, what is sharding? You can run Hashgraph in a single [01:03:30] network where every node knows everything, every node processes every transaction, they're all exactly identical, they're only there to keep each other honest, this is how a permission network often works. This is how Hedera on day one will be working for obvious reasons. By the way it's working right now, we have a test network crossing three continents at the moment. I'm expecting the fourth continent to come online soon. But that's how you expect it to start, is one network where everybody has the same data. It is obvious-

Demetri Kofinas: Single shard.

Leemon Baird: [01:04:00] Exactly. We call that a sharding. Well yes, it's a degenerate case of one shard. It is obvious to everybody that ultimately you want to get even faster. You want the network to handle more transactions per second than a single computer can physically grab over the internet. No computer connects to the internet fast enough to get all the transactions you want to do. You want to hundreds of thousands, you want to do millions, you want to do billions, you want to trillions, clearly one computer can't handle that. So you cannot [01:04:30] have every computer handling every transaction, you have to break them up to pieces. There's no question about that. If you have a big sheet of glass and you break it up into pieces what you call the pieces of glass? You call them shards.

More importantly in the database world for decades, when you take a big database and you store each piece of the database on several computers but not all the computers, they're called shards. This is what sharding is. So it's clear that a ledger, a public ledger, a big public ledger especially you go [01:05:00] to millions of nodes wants to have multiple shards, no question. And that means we're going to take our million computers and break them up into groups of a few hundred. Why a few hundred? Well that's enough to be secure and not overkill, I don't want to put a million into one shard because that's a waste. I might as well take most of those million to make more shards, it gives me more speed, I like that.

So it is obvious that you want to break up into shards. What is not always obvious to people though is that, that's not enough, you also [01:05:30] have to make each shard fast. That's not obvious in a lot of ways, but this is critically important. There are cases where lots of transactions all have to talk to the same shard and it's impossible for various mathematical reasons to eliminate that entirely. So for some use cases, everybody's talking to one shard, that shard needs to be really fast. In other use cases, stuff is going on in this shard and stuff is going on this shard and they're completely unrelated to each other and no one cares, and so we run twice as fast with two shards as we would [01:06:00] have with one. Yeah, we win. And if we have a million shards, we run a million times faster, if everything is completely independent. And in real life, your applications will be somewhere in between.

A million shards will be somewhere between a million times faster and one times faster, somewhere in the middle and different applications will be at different places on that

spectrum. So you want speed and you want shards. Now the question is how should we do our sharding? Many people have suggested ways of [01:06:30] doing sharding which are not exactly everyone being equal. We're getting back to this decentralized theme. This seems to be a theme today, everything we talk about comes back to decentralization, they say we're going to be decentralized in the sense of having lots of shards, one of which is the master shard that has to hold all the information and eventually all the information has to trickle back to the master shard.

Demetri Kofinas: Not really decentralized.

Leemon Baird: Not really decentralized. And here we're not worried about security we're worried about speed. Other people have said, "We'll really decentralize it. We'll trust things that [01:07:00] maybe isn't actually trustworthy and it's conceivable that we could end up with double spending happening or data lost or malicious things happening." That's also not good. What you want in a single shard is asynchronous BFT with speed. What you want in a bunch of shards together, is Asynchronous Byzantine Fault Tolerance with speed. You want ABFT of the whole system. That's what we have.

Mathematically [01:07:30] guaranteed, I don't trust things if they aren't proven, by the way we actually have now this beautiful project where we're using computers to prove that our proofs are right, because I don't even trust a human being like myself writing math proofs on paper in English, I want a computer to check it. What we have is an ABFT system that is fast. There is no one shard that holds all the information or that all the information has to coordinate with. Instead, we do the following, if you would [01:08:00] like to hear an example of how you would do both sharding with our system.

Demetri Kofinas: Sure.

Leemon Baird: Here's the bedrock of our system, we will have to trust each shard to be trustworthy. That means it has to be big enough and has to be running Hashgraph, so that makes it ... as long as no one third is bad then we're okay and we do all the things we talked about to make each shard individually secure. And then the Shards can trust each other, then we have the shards send messages to each other. Notice [01:08:30] I didn't say the computers are sending messages to each other, I said the shards are sending messages to each other. This group of hundreds of computers is itself one thing that in some sense can think and send messages. And this shard is a thing [crosstalk 01:08:45].

Demetri Kofinas: It's pretty cool. It's pretty cool.

Leemon Baird: Isn't that cool?

Demetri Kofinas: Yeah.

Leemon Baird: It's kind of cool.

Demetri Kofinas: Kind of cool.

Leemon Baird: So this shard can send this shard, ultimately, it's one of the pieces of this shard, the individual computers, randomly chooses itself, randomly chooses [01:09:00] one of these and hands it the message. But it doesn't just hand it the message, it hands it a state proof. A little tiny proof that says, "This isn't just my opinion, this is the consensus of my shard. It's official." And then this other guy says, "Okay, I believe you," and if he's malicious he ignores you and doesn't do anything. But he's a good guy and you'll just keep trying until you reach a good guy at random, and most of them are good guys.

Demetri Kofinas: Because you're getting pushed out, right?

Leemon Baird: It's push.

Demetri Kofinas: It's push.

Leemon Baird: Messages are all push, never pull. [01:09:30] Always push. If you have a million shards, pull will be bad, have to be pulling for a million shards. It's always push, this will be randomly trying to push a message and this one will then tell all of the people in his community, "Hey, we just got a message from that Shard over there, here's the message and here's the state proof proving it's an official message from the shard, not from some random computer but from the shard itself." And when they all reach consensus on where in history it is, they execute [01:10:00] it. So how would this work with cryptocurrency transactions? Here we go. Alice wants to send Bob some cryptocurrency, she creates a transaction that says, "I Alice, hereby authorize 10 coins to be transferred from my account to Bob's account," and digitally signs it.

Maybe she's just a client, she's not even on node or anything. But Alice then would call one random computer that's a node in the shard holding her account. Each account is only in one shard and they're all in different shards. [01:10:30] And says, "Please send the money to Bob." Now if we're lucky, Bob is also in the same shard. And so the shard now just acts exactly like a single network that wasn't sharded, it reaches consensus, at the moment where it reaches consensus it checks, "Okay, does Alice actually have 10 coins?" At this moment in history if she has 10 coins we'll let it go through and we'll detriment her by 10 coins and increment Bobby 10 coins, just change two numbers in memory, really trivial. The hard part was checking the signature and that we do in the GPU at a million a second.

Demetri Kofinas: That brings us back to the point.

Leemon Baird: That [01:11:00] brings us back. But she then has 10 subtracted, he has 10 added. Every single node does this at the same time, just purely locally it changes of the two numbers in memory, they'll change it the same way. They digitally sign their state and gossip it so that we all know about, everybody agreeing and that's what happens, very straightforward, very fast. That's the consensus latency we've been talking about. Now, if Carol sends to Dave, and they're both in this shard, we have the [01:11:30] same thing, everything's good. What if Alice wants to Dave? Two different shards, Alice will send her transaction just like before.

She doesn't even have to know what shard Dave is in, although actually it's part of the name of the account. Tells what shard. But Alice just says, “I want to send money to Dave.” She sends it to a random node in her shard, it's digitally signed. The shard comes to conclusion and then it says, when it knows exactly where in history [01:12:00] it is, it says, "Okay, we will now officially approve that she has at least 10 coins in her account, we're going to decrement her account by 10 coins and we're going to create an official message from the shard saying, 'Please add 10 coins to Dave.'" With the process I just said, eventually it gets transferred by some random computer, they keep randomly nominating themselves to push, there's no one person in charge and they each pick [01:12:30] a random computer.

There's no one person that can stop it, eventually it'll get through, it'll get put into their ledger, they'll get consensus on it, it will have a pointing consensus history and they will all say, “I can't see Alice's account. I don't know that it was decremented but you know what? We have a cryptographic proof that the entire Alice shard as a whole approved this and agrees that they have decremented Alice and we trust them, so we believe that her account was decremented. We're going increment Bob and Dave.” [01:13:00] And they do it. And because we can trust each other and because we have proofs that we had consensus, the total number of coins in the universe does not change.

Demetri Kofinas: So you're able to have a fully sharded solution that still comes to network wide consensus.

Leemon Baird: Yes.

Demetri Kofinas: Which is what allows this entire ... Sort of the applications we've been talking about.

Leemon Baird: Yes. The entire network is Asynchronous Byzantine Fault Tolerant as long each shard is Asynchronous Byzantine Fault Tolerant, and the entire [01:13:30] network is going to be fast, because there's no one shard that holds everybody's account. You could have the accounts temporarily in these shards but then there's the one master shard that has all the accounts, and at the end of the day we all send the totals to that one, that's bad on multiple counts, most of which is that eventually all these transactions have to go to the central one and for some flow patterns, that can overwhelm you, or there has to be trust going on in ways that isn't good, which will also overwhelm you. There's lots of bad things that can happen with side chains if they're not done in the right ways. What we have is not side chains [01:14:00] because they're not chains and they're not side, side implies there's a main and then the non-main, we're all the same. We're decentralized.

Demetri Kofinas: Well that brings us back though to the Hashgraph consensus protocol, all this is possible because of Hashgraph and these were conversations that we had early on before we were able to have this conversation about Hedera in our last interviews. And that was always something that you alluded to, whether it was to me or to the audience which was that, there are things that you're going to be able to do to create a

public ledger that you wouldn't be able to [01:14:30] implement otherwise because of the fact that you have this consensus protocol, that is fast and secure.

Leemon Baird: Yes.

Demetri Kofinas: And you're here now.

Leemon Baird: It is. Yes, for two years people have being saying, "What about that public ledger?" And I've been saying, "Well you know, we want to do a thing ..." It's all about doing things in the right order, we wanted to prove it out as a permission but now we have the public ledger and it's Asynchronous BFT because the individual shards Asynchronous BFT and why are they that? Because Hashgraph is that.

Demetri Kofinas: So Leemon you have indulged [01:15:00] me and our audience for a tremendous amount of time here. I want to make sure that ... there's going to be so much obviously that we can't get to. And this interview have come out right after your presentation, hopefully we'll have it right up afterwards. There will be a white paper that will be out, you will be adding to that white paper, you will be making adjustments to the code, people will be learning more about this. I guess I want to sort of put a bow on this conversation [01:15:30] for people who are interested, who want to understand what they can expect in the next month or two or three as far as developing, are you going to have open APIs? When are you going to have those? Where can people look to find more information? Because this is actually it, like we were dancing around this for months, since I found your white paper in September. I mean this is it, you're launching the public ledger, so what's next?

Leemon Baird: Yes. So we have a running network right now, I have a wallet software on phone but these are all early versions, [01:16:00] they will become more secure, they will become more feature. We will test them, we do not want to release things before they are ready that's why earlier we were just doing the permissions stuff. We wanted to test it out first and get market traction and have proof of concept and show that it's working, not just proof of concept but actually working. We're going to do the same thing with Hedera, we're going to do it the right way. It's going to be pretty fast though I think. We will go through the steps of internal testing and then testing with our members that are in our advisory members, then testing with a small developer group, and then testing [01:16:30] with a bigger developer group. At some point what I just called testing turns into ... Well yeah, you're testing but it's with real cryptocurrency. And then at some point we will be selling, who knows?

Demetri Kofinas: You know everyone's thinking when [crosstalk 01:16:43].

Leemon Baird: I know, I know, I know, I know.

Demetri Kofinas: I've seen all that on the Telegraph channel, everyone keeps asking "When ICO"

Leemon Baird: When ICO. So people will continue to ask that. So the short answer is, it will all happen at the appropriate time. The long answer is, we're pushing everything to happen on as fast [01:17:00] a schedule as we can while being secure, it has to be secure. And if you want to know go to Hashgraph.com and sign up and we will email you each of these steps.

Demetri Kofinas: It's also not an ICO to be fair, right? In other words you're not ... This is not of the model that sort of typical for the community, so I think that, that's also ... People have a framework for understanding this type of technology that's based on the legacy sort of architecture that already exists, but your approach has been very new, whether we're talking about governance, whether we're talking [01:17:30] about open review versus open source. And whether we're talking about the coins and whether ... The fact that there's no emphasis and there hasn't been from the beginning of the coins that has ironically frustrated so many people, because like people are dying to buy something that they don't understand, and there's so much to understand here.

Leemon Baird: So you're right. We're different in every way. We're different in what we treat the cryptocurrency, we're different in ICO, we're different in governance and the reason is ... Okay. The bottom line is, [01:18:00] we're trying to build something real that will last for 100 years and will become the utility for the planet.

Demetri Kofinas: That's a big deal.

Leemon Baird: It is a big deal and I won't say there's anyone out there who's focused on just, "Let's have an ICO today and then we'll get money." Conceivably there might even be people that have ICOs for that sort of reason. Our goal from the beginning-

Demetri Kofinas: For sure.

Leemon Baird: ... Has been, we want to build a real thing that will last for 100 years, that has governance done right, that has cryptocurrency done right, that has [01:18:30] the services done right, that is being done in a measured correct way so that you'll have fast, fair and secure at every level of the system that you'll have governance that prevent splitting, that makes it governed right, that can comply with government regulation, that has privacy, all those things done right. This has been our goal from the beginning. We're going to move out as fast as we can, but not any faster than that. We're not going to move out faster than we ought to, and if you sign up with Hashgraph.com, you can find out as we're moving, we'll keep you in [01:19:00] the loop.

Demetri Kofinas: And I do want to emphasize that point because the approach that you've taken from the first day I met you, I mean I read your paper in September and you didn't fit the mold for sure. This process has been for me about also kind of letting go, we're trying not to have biases around how I think about Hashgraph and what you're trying to do. It's a great approach. We certainly didn't do [01:19:30] the governance conversation justice or anything on the regulatory front. I do suggest to everyone that's watching this interview to go online go to Hashgraph ... Is it Hashgraph.com? Is that ...

Leemon Baird: Go to Hashgraph.com.

Demetri Kofinas: ... .com and download the white paper, check out sort of how you guys do regulations, how you do governance. Leemon, I thank you so much for coming and I appreciate you taking the time to do it.

Leemon Baird: Thank you, I really appreciate it, this has been fun, thank you.

Demetri Kofinas: And [01:20:00] that was my episode with Leemon Baird. And I want to thank Leemon for being on my program. Today's episode was produced by me and edited by Stylianos Nicolaou. For more episodes, you can check out our website at HiddenForces.io. Join the conversation through Facebook, Twitter and Instagram @HiddenForcesPod or send me an email. Thanks for listening, we'll see you next week.